UNIDIR

O que é necessário para construir capacidades cibernéticas?

Parte I. Classificação das Capacidades Cibernéticas Fundamentais

SAMUELE DOMINIONI · GIACOMO PERSI PAOLI

Obrigado

Pelo apoio dos principais contribuintes do UNIDIR que sustentam todas as atividades do Instituto. Este estudo faz parte do fluxo de trabalho de estabilidade cibernética do Programa de Segurança e Tecnologia UNIDIR, financiado pela Microsoft e pelos governos da República Tcheca, França, Alemanha, Itália, Holanda, Suíça e Reino Unido.

O UNIDIR deseja expressar sua gratidão ao Programa de Segurança Cibernética do Comitê Interamericano contra o Terrorismo (CICTE) da Organização dos Estados Americanos (OEA) por traduzir esta pesquisa e disponibilizá-la em português. Este relatório foi inicialmente publicado em julho de 2023 em inglês, que permanece a versão oficial. Em caso de divergência, o texto em inglês prevalecerá.

Sobre UNIDIR

O Instituto das Nações Unidas para Pesquisa de Desarmamento (UNIDIR) é um instituto autônomo das Nações Unidas financiado por contribuições voluntárias. O UNIDIR, um dos poucos institutos de políticas do mundo com foco no desarmamento, gera conhecimento e promove o diálogo e a ação sobre desarmamento e segurança. Com sede em Genebra, o UNIDIR auxilia a comunidade internacional no desenvolvimento de ideias práticas e inovadoras necessárias para encontrar soluções para problemas críticos de segurança.

Observação

Os Autores

Samuele Dominioni

Pesquisador, Programa de Segurança e Tecnologia

O Dr. Samuele Dominioni é pesquisador do Programa de Segurança e Tecnologia da UNIDIR. Antes de ingressar na UNIDIR, ocupou cargos de pesquisa em ambientes acadêmicos e de grupos de especialistas. É PhD em relações internacionais e história política pela Sciences Po, na França, e pela Escola de Estudos Avançados do IMT, na Itália.

Giacomo Persi Paoli

Diretor do Programa, Segurança e Tecnologia

O Dr. Giacomo Persi Paoli é o Diretor do Programa de Segurança e Tecnologia da UNIDIR. Seu conhecimento especializado abrange ciência e tecnologia com ênfase nas implicações de tecnologias emergentes para segurança e defesa. Antes de ingressar na UNIDIR, Giacomo foi Diretor Associado da RAND Europe, onde liderou o portfólio de ciência, tecnologia e inovação de defesa e segurança, bem como o Centro de Estudos de Prospecção da RAND. Ele é Ph.D. em Economia pela Universidade de Roma, Itália, e mestre em Ciência Política pela Universidade de Pisa, Itália.

Tabela de Conteúdo

Abreviações e Acrônimos		**5**
Sumário Executivo		**6**
1.	**Introdução**	**9**
	Nota sobre a Metodologia	11
2.	**Introdução aos Recursos Cibernéticos Fundamentais**	**12**
3.	**Detalhamento da FCC: Normas de Comportamento Responsável dos Estados**	**15**
3.1	Norma A	18
3.2	Norma B	21
3.3	Norma C	23
3.4	Norma D	25
3.5	Norma E	27
3.6	Norma F	29
3.7	Norma G	31
3.8	Norma H	33
3.9	Norma I	35
3.10	Norma J	37
3.11	Norma K	40
4.	**Desglose de las FCC: Direito Internacional**	**42**
5.	**Desglose de las FCC: Medidas de Fortalecimento da Confiança**	**44**
6.	**Conclusões**	**47**
Anexo 1. Tabela de Capacidades Cibernéticas Fundamentais		**49**

Abreviações e Acrônimos

CERT/CSIRT	Equipe de Resposta a Emergências Informáticas/Equipe de Resposta a Incidentes de Segurança Informática
DCV	Divulgação de vulnerabilidade coordenada
FCC	Capacidades Cibernéticas Fundamentais
GEG	Grupo de Peritos Governamentais
GTCA	Grupo de trabalho aberto (OEWG)
MFC	Medidas de construção de confiança
TIC	Tecnologia da informação e comunicação
UNIDIR	Instituto das Nações Unidas para Pesquisa de Desarmamento
UNODA	Escritório das Nações Unidas para Assuntos de Desarmamento
VEX	Compartilhamento de exploração de vulnerabilidade

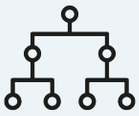
Sumário Executivo

Nas últimas duas décadas, os Estados têm explorado ativamente formas de garantir a paz e a segurança internacional no campo das Tecnologias de Informação e Comunicação (TIC). Esses esforços resultaram na adoção, pela Assembleia Geral, de um conjunto de medidas conhecidas coletivamente como o Marco das Nações Unidas para o Comportamento Responsável do Estado no Ciberespaço (doravante o Marco), que define o que os Estado-membros devem e não devem fazer no ambiente das TIC em uma perspectiva de segurança internacional. O Marco baseia-se nos componentes fundamentais da criação de capacidades específicas: 11 normas voluntárias e não vinculativas de comportamento responsável do Estado, medidas de fortalecimento da confiança e direito internacional.

No OEWG em andamento (2021-2025), muitos Estado-membros salientaram a necessidade de apoiar a implementação do Marco por meio, entre outros aspectos, de orientações, assistência e esforços de criação das capacidades. O presente relatório é a primeira parte de um estudo realizado pelo UNIDIR destinado a apoiar os Estados em seus esforços para implementar o Marco e aumentar a sua cibersegurança e resiliência.

Em particular, este relatório identifica as *capacidades cibernéticas fundamentais* (FCC), definidas como a combinação de políticas e regulamentos, processos e estruturas, parcerias e redes, pessoas

e habilidades, e as tecnologias **consideradas necessárias** para implementar **cada elemento do Marco**: as 11 normas, direito internacional e medidas de fortalecimento da confiança.

Políticas e Regulamentos 	Documentos oficiais relacionados a questões de cibersegurança. Estes incluem documentos que descrevem as posições, políticas e estratégias (desenvolvidas especificamente para setores-chave, por exemplo, infraestrutura crítica ou para aplicações intersetoriais em nível nacional) dos Estado-membros, bem como marcos legais e regulamentares e assinatura de acordos ou outros instrumentos de cooperação com as partes interessadas internacionais.
Processos e Estruturas 	Cargos-chave, órgãos ou entidades responsáveis, outros mecanismos nacionais ou regionais e processos, procedimentos e protocolos oficiais relacionados com a cibersegurança.
Associações e Redes 	Iniciativas, tanto a nível nacional como internacional, destinadas a fortalecer as capacidades nacionais. A nível nacional, trata-se de mecanismos ou instrumentos de cooperação intrassetorial e intragovernamental. A nível internacional, mecanismos ou instrumentos de cooperação bilateral, regional e multilateral.
Pessoas e Habilidades 	Conhecimento e experiência especializada em cibersegurança. Note-se que algumas FCC listadas no pilar “pessoas e competências” poderão também ser cumpridos através da terceirização e do estabelecimento de acordos com provedores externos ou outras partes interessadas quando o Estado não puder desenvolver ou manter internamente as capacidades especializadas.
Tecnologia 	Soluções e capacidades técnicas a nível nacional relacionadas com a cibersegurança. Deve-se notar que as FCC listados no pilar “tecnologia” também podem ser atendidos por terceirização para prestadores de serviços externos por meio, por exemplo, de parcerias público-privadas.

É importante notar que as FCC se destinam a atuar como condições iniciais a partir das quais podem ser desenvolvidas respostas mais refinadas e abrangentes uma vez que essas condições iniciais sejam atendidas. Portanto, os FCC representam os requisitos de capacidade “mínimos” necessários para a implementação do Marco, e não as melhores soluções ou os requisitos de capacidade “ótimos”.

O conjunto de FCC pode ser utilizado como uma ferramenta para melhor identificar os requisitos e a priorização das intervenções de desenvolvimento de capacidades com base nas necessidades e contextos específicos nacionais específicos, fortalecendo assim os vínculos entre a implementação do Marco e os debates relacionados à capacitação, incluindo aquelas que têm lugar no atual OEWG (e potenciais futuros Programas de Ação).

1. Introdução

A área de tecnologia da informação e comunicação (TIC) mudou e evoluiu ao longo das décadas, expandindo-se para abranger quase todas as diferentes facetas da atividade humana. As Nações Unidas reconheceram que hoje as TIC "têm implicações para [...] paz e segurança, direitos humanos e desenvolvimento sustentável. As TIC e a conectividade global têm sido um catalisador para o progresso e o desenvolvimento humano, transformando sociedades e economias e expandindo as oportunidades de cooperação.[1] Junto com a crescente relevância das TICs em diferentes setores, múltiplos esforços também foram feitos nas últimas décadas para estabelecer marcos regulatórios para as TICs.

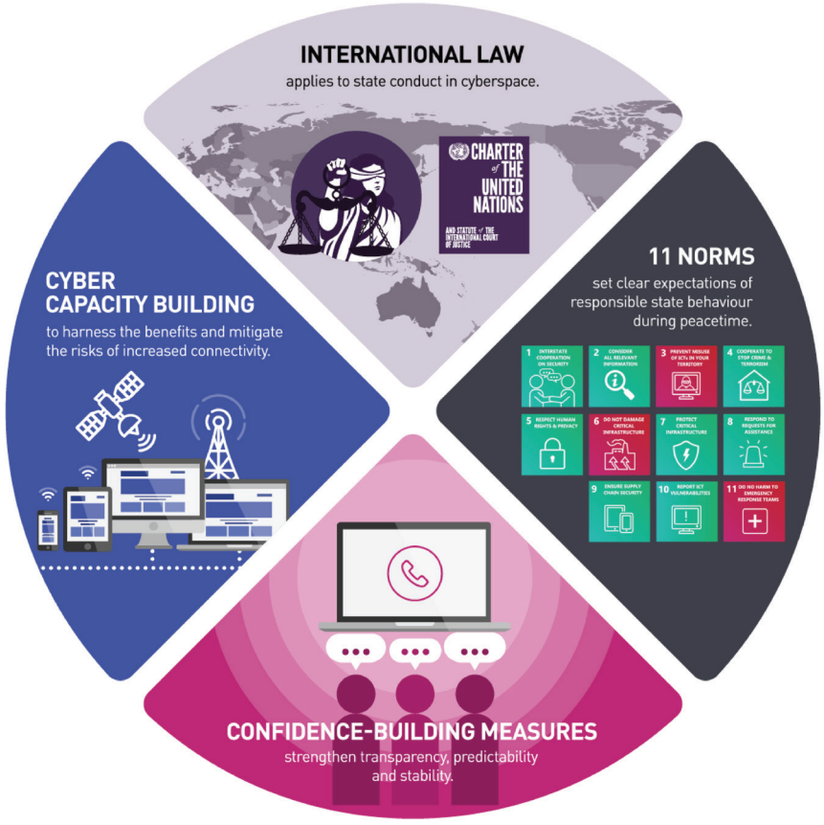
Entre esses esforços para regular o campo das TIC encontra-se o Marco para o Comportamento Responsável dos Estados (doravante, o Marco), que define o que os Estado-membros devem e não devem fazer no ambiente das TIC em uma perspectiva de segurança internacional. O Marco é o resultado de cerca de duas décadas de negociações (em diferentes formatos) nas Nações Unidas. Em particular, baseia-se no relatório do Grupo de Trabalho Aberto (OEWG) de 2021 sobre os desenvolvimentos no campo das TIC no contexto da segurança internacional e nos relatórios de consenso dos Grupos de Peritos Governamentais (GEG) de 2010, 2013, 2015 e 2021.

---

1 **OEWG. 2021. Final Substantive Report**, parágrafo 2.

Nestes relatórios, de natureza cumulativa, os Estados-membros elaboraram 11 normas voluntárias não vinculativas relacionadas ao comportamento responsável dos Estados, recomendaram medidas específicas para o fortalecimento da confiança, criação de capacidades e de cooperação e determinaram que o Direito Internacional, em particular a Carta das Nações Unidas como aplicável e essencial para manter a paz, a segurança e a estabilidade no ambiente de TIC. Estes três elementos (normas, direito internacional e medidas de fortalecimento da confiança), apoiados pela criação de capacidades, constituem o Marco (ver Figura 1).

Figura1. Marco das Nações Unidas para o Comportamento Responsável do Estado no Ciberespaço



Fonte: **https://www.internationalcybertech.gov.au/un-cyber-norms-resources**

No OEWG em andamento (2021-2025), muitos Estados-membros destacaram a necessidade de apoiar a implementação da Estrutura por meio, entre outros aspectos, de orientações, assistência e esforços dedicados à capacitação. Em resposta a esta demanda e com o objetivo de aumentar a cibersegurança e a resiliência dos Estado-membros, o UNIDIR realizou pesquisas com três objetivos principais:

1. Identificar as Capacidades Cibernéticas Fundamentais (FCC) que são consideradas necessárias para implementar o Marco de forma eficaz.
2. Fortalecer os vínculos entre o Marco e a capacidade dos Estados de prevenir ou mitigar efetivamente o impacto de atividades maliciosas de TIC.

3. Desenhar uma ferramenta para identificar melhor os requisitos e priorizar as intervenções de capacitação com base nas necessidades e contextos específicos de cada país, fortalecendo assim os vínculos entre a implementação da Estrutura e as discussões relacionadas à capacitação, incluindo aquelas que ocorrem no atual OEWG (e possíveis futuros programas de ação).

Este relatório está centrado no objetivo 1, contribui para o objetivo 3 e fornece a base para a abordagem do objetivo 2, que é objeto de uma publicação separada.[2]

Nota Sobre a Metodologia[3]

A pesquisa foi realizada em duas fases com uma abordagem de métodos mistos. A primeira centrou-se na identificação das chamadas FCC, que são definidas como a combinação de políticas e regulamentos, processos e estruturas, parcerias e redes, pessoas e competências e tecnologias consideradas necessárias para implementar o Marco (ver definições no Capítulo 2). Esta fase envolveu uma revisão documental de todos os relatórios acordados no primeiro OEWG (2021) e produzidos pelos Grupos de Peritos Governamentais em Cibersegurança (2010, 2013, 2015 e 2021) e literatura adicional. Posteriormente, foram realizadas entrevistas estruturadas com diplomatas e especialistas em cibersegurança de Estados-membros selecionados e outras partes interessadas (incluindo a sociedade civil e o setor privado).[4] Pesquisa documental e um conjunto de entrevistas preliminares foram utilizados para gerar uma lista inicial de FCC. A segunda fase da investigação consistiu em testar a lista das FCC contra ameaças cibernéticas específicas (ransomware, ataque distribuído de negação de serviço (DDOS) e manipulação da cadeia de abastecimento);[5] para tanto, foram realizados dois workshops com cenários baseados em ameaças (um interno e outro com especialistas externos).[6] Os dados resultantes dos dois workshops foram agregados e analisados. O UNIDIR apresentou os resultados preliminares do projeto de investigação em um evento paralelo à quarta sessão do OEWG em Nova York (6 a 10 de março de 2023). Finalmente, para refinar os resultados, foi realizada uma rodada final de consultas com especialistas externos.

---

2 Ver Samuele Dominioni y Giacomo Persi Paoli. 2023. Unpacking Cyber Capacity-Building: Part II. Introducing a Threat-Based Approach. UNIDIR.

3 Agradecemos aos Estado-membros e organizações que participaram do projeto de pesquisa: Argentina, Austrália, República Tcheca, Dinamarca, Estônia, Gana, Israel, Itália, Quênia, Jamaica, Malásia, Ilhas Maurício, México, Holanda, Cingapura e Reino Unido; e FIRST, Global Forum for Cyber Expertise, INTERPOL, International Chamber of Commerce, Royal United Services Institute, Kaspersky, Microsoft e a Escola de Estudos Internacionais de Rajaratnam (RSIS).

4 A diversidade geográfica e de gênero foi levada em consideração na seleção dos entrevistados.

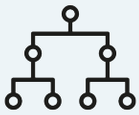
5 A seleção foi feita considerando as ameaças frequentemente mencionadas nas discussões multilaterais.

6 Workshops de especialistas externos e internos foram alternados com sessões plenárias e grupos de trabalho para analisar, com o apoio de cenários específicos, os três estudos de caso com vista a associar os elementos relevantes do Marco com FCC específicos e necessidades relevantes. Por exemplo, usando ransomware como ponto de entrada, os participantes do workshop analisaram o Marco para identificar as normas, as leis internacionais ou CBM relevantes que podem se aplicar ao cenário. Posteriormente selecionaram as FCC mais adequadas para enfrentar a ameaça.

2. Introdução às Capacidades Cibernéticas Fundamentais

As FCC são definidas como a combinação de políticas e regulamentos, processos e estruturas, parcerias e redes, pessoas e competências e tecnologias consideradas necessárias para implementar o Marco. Para efeitos deste estudo, estes cinco pilares são definidos da seguinte forma:

Tabela 1. Os Cinco Pilares para a Implementação do Marco

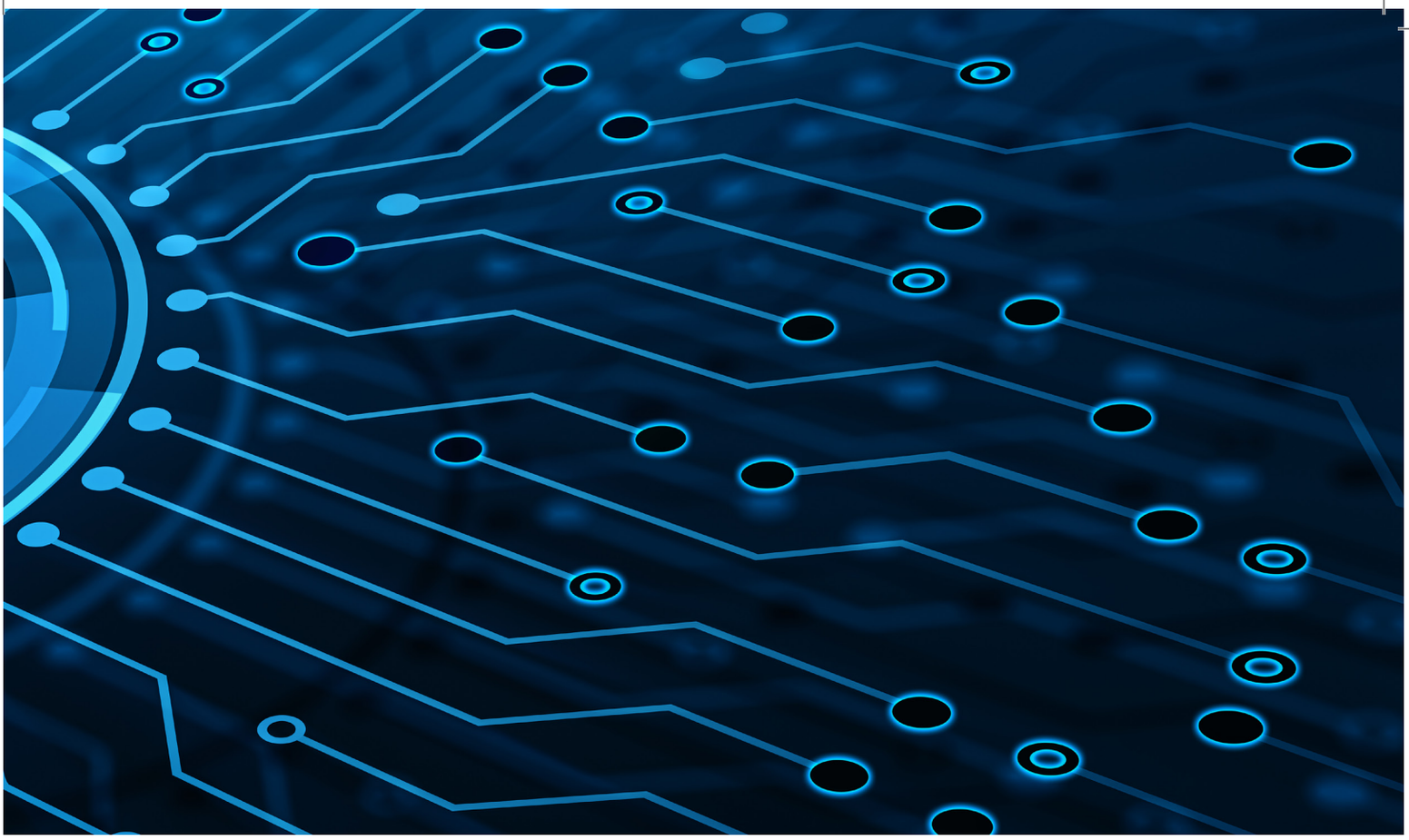
Políticas e Regulamentos 	Documentos oficiais relacionados a questões de cibersegurança. Incluem documentos que descrevem as posições, políticas e estratégias (desenvolvidas especificamente para setores-chave, por exemplo, infraestrutura crítica ou para aplicações intersetoriais em nível nacional) dos Estados-membros, bem como marcos legais e regulamentares e assinatura de acordos ou outros instrumentos de cooperação com as partes interessadas internacionais.
Processos e Estruturas 	Cargos-chave, órgãos ou entidades responsáveis, outros mecanismos nacionais ou regionais e processos, procedimentos e protocolos oficiais relacionados com a cibersegurança.
Associações e Redes 	Iniciativas, tanto a nível nacional como internacional, destinadas a fortalecer as capacidades nacionais. A nível nacional, trata-se de mecanismos ou instrumentos de cooperação intrassetorial e intragovernamental. A nível internacional, mecanismos ou instrumentos de cooperação bilateral, regional e multilateral.
Pessoas e Competências 	Conhecimento e experiência especializada em cibersegurança. Note-se que alguns FCC incluídos no pilar “pessoas e competências” poderão também ser satisfeitos através da terceirização e do estabelecimento de acordos com provedores externos ou outras partes interessadas quando o Estado não puder desenvolver ou manter internamente as capacidades especiais.
Tecnologia 	Soluções e capacidades técnicas à escala nacional relacionadas com a cibersegurança. Deve-se notar que os FCC incluídos no pilar “tecnologia” também podem ser atendidos por terceirização ou prestadores de serviços externos por meio, por exemplo, de parcerias público-privadas.

É importante observar que o objetivo das FCC, desenvolvidos com a metodologia descrita no Capítulo 1, é representar os recursos essenciais ou necessários para implementar o Marco. A lista da FCC não pretende ser representativa das melhores práticas ou medidas desejáveis. Eles foram desenvolvidos com a ideia de que atuam como as condições iniciais a partir das quais respostas mais refinadas e abrangentes podem ser desenvolvidas uma vez que essas condições iniciais sejam atendidas. Portanto, as FCC representam os requisitos mínimos de capacidade necessários para a implementação do Marco e não as soluções ótimas ou respostas ideais. Por esta razão, os elementos que não surgiram como verdadeiramente necessários ou fundamentais não foram incluídos na lista por terem um caráter mais aspiracional, desejável ou “avançado”.

Também é importante notar que mais ênfase é colocada em qual capacidade deve estar presente do que em como desenvolvê-la, um aspecto que continua sendo uma prerrogativa de cada país. Alguns exemplos de “como fazer” são fornecidos neste relatório, mas apenas para fins de orientação e ilustração.

Por último, o objetivo das FCC identificadas é orientar os Estado-membros na implementação do Marco e podem ser consideradas elementos importantes, até mesmo necessárias, para alcançar maior maturidade nos acordos nacionais de cibersegurança. No entanto, focar apenas no Marco não será suficiente para garantir a abrangência da preparação e resiliência cibernética. Nesse sentido, este estudo complementa – em vez de repetir ou substituir – as abordagens existentes concebidas para o propósito específico de avaliar a preparação ou maturidade cibernética geral de cada país.

O Anexo 1 fornece uma visão geral dos recursos relacionados a cada componente do Marco e os Capítulos 3-5 descrevem-nas mais pormenorizadamente.



3. Detalhamento das FCC: Normas de Comportamento Responsável dos Estados

Esta seção descreve as capacidades cibernéticas fundamentais necessárias para implementar as 11 normas não vinculativas de comportamento responsável dos Estados no campo das TIC (ver Figura 3). O capítulo está estruturado de forma que cada norma possa ser lida de forma independente dependendo dos interesses específicos de cada leitor. Alguns FCC podem aparecer em várias normas, às vezes como repetições exatas ou com descrições mais sutis, dependendo da norma. Estas normas foram endossadas pela Assembleia Geral das Nações Unidas por meio da adoção da resolução 70/237 em dezembro de 2015. Essa resolução instou os Estado-membros a serem guiados pelas 11 normas não vinculativas propostas pelo quarto GEG. Em 2021, o relatório final do sexto GEG acrescentou informações adicionais sobre essas normas e reafirmou seu valor para orientar o comportamento responsável dos Estados no ciberespaço. O relatório substantivo do primeiro OEWG de 2021 também reconheceu e reafirmou as 11 normas não vinculativas.

Figura 2. Regras de Comportamento Responsável dos Estados no Ciberespaço

Fonte: https://www.internationalcybertech.gov.au/un-cyber-norms-resources

Devemos notar que algumas normas devem ser consideradas essenciais e transversais e, por conseguinte, aplicáveis em todos os cenários e uma condição prévia para a implementação de todas as outras. É o caso da Norma A,[7] que lista os requisitos gerais que sustentam a cooperação interestadual, e da Norma E,[8] que se centra no respeito e na proteção dos direitos humanos.

Além disso, expandindo o que o relatório do GTCA de 2021 afirma – "a criação de capacidades deve respeitar os direitos humanos e as liberdades fundamentais, ser inclusiva e sensível às questões de gênero, universal e não discriminatória"[9]– Recomenda-se que os Estados-membros, ao implementarem as capacidades identificadas pelo Marco, considerem as formas pelas quais essas capacidades podem afetar de forma diferente as dimensões do gênero, incluindo as brechas de gênero entre

7 "De acordo com os propósitos das Nações Unidas, incluindo a manutenção da paz e segurança internacional, os Estados devem cooperar no desenvolvimento e aplicação de medidas para aumentar a estabilidade e segurança no uso das TIC e prevenir práticas de TIC reconhecidas como prejudiciais ou que possam representar ameaças à paz e segurança internacionais.

8 "Os Estados, ao garantir o uso seguro das TICs, devem respeitar as resoluções 20/8 e 26/13 do Conselho de Direitos Humanos relacionadas à promoção, proteção e gozo dos direitos humanos na Internet, bem como as resoluções 68/167 e 69/166 da Assembleia Geral sobre o direito à privacidade na era digital, a fim de garantir o pleno respeito aos direitos humanos, incluindo o direito à liberdade de expressão".

9 OEWG. 2021. Relatório substantivo final, par. 56.

os ciberprofissionais,[10] as respostas jurídicas com perspectiva de gênero para incidentes cibernéticos[11] e os impactos de incidentes maliciosos[12] e suas respostas.[13] Por outro lado, no atual OEWG, um número crescente de Estados reconheceu a importância de aplicar uma perspectiva de gênero nas discussões, em particular promovendo o compartilhamento sobre os impactos de gênero dos incidentes de TIC e reduzindo a brecha digital entre gêneros. Diante desse interesse crescente, pesquisas futuras poderiam ser realizadas para orientar a incorporação da perspectiva de gênero em todos os componentes do marco de comportamento responsável dos Estados.

10 Ver Katharine Millar, James Shires, Tatiana Tropina. 2021. Gender Approaches to Cybersecurity: Design, Defence and Response. UNIDIR.

11 Ibid.

12 Ver Deborah Brown e Allison Pytlak. 2020. Why Gender Matters in International Cyber Security. Women's International League for Peace and Freedom and the Association for Progressive Communications.

13 Sérgio Drozo. 2021. Diversity and Cyber Resilience: Views of an Incident Responder. UNIDIR.

3.1 Norma A

De acordo com os propósitos das Nações Unidas, incluindo a manutenção da paz e segurança internacional, os Estados devem cooperar no desenvolvimento e aplicação de medidas para aumentar a estabilidade e segurança no uso das TIC e prevenir práticas de TIC reconhecidas como prejudiciais ou que possam representar ameaças à paz e segurança internacionais.

Políticas e Regulamentos

Considerando o amplo espectro de possíveis ações que os Estado-membros podem tomar para implementar esta norma, recomenda-se fazer **uma interpretação nacional da norma** antes de tomar qualquer outra ação. Ao pensar cuidadosamente sobre como implementar esta norma a nível nacional, os Estados-membros podem refletir sobre como cooperar com outras partes interessadas para cumprir os objetivos descritos na norma. Posteriormente, o essencial seria a adoção de uma **política, estratégia ou legislação de cibersegurança** que descreva os princípios e objetivos (e o respetivo plano de implementação).[14] É particularmente importante que a política ou estratégia assuma uma abordagem de todo o governo, o que implica a possibilidade de ação em todos os níveis de governo. Além disso, os Estados-membros devem definir **uma abordagem de gestão do risco cibernético** (incluindo infraestrutura crítica) que inclua a cooperação com outras partes interessadas.

Para promover medidas de cooperação em nível internacional, são recomendadas declarações públicas que reconheçam **a cibersegurança como uma das prioridades da política externa**, um **compromisso público com o Marco** e como ele se aplica ao uso das TIC pelos Estados. Uma declaração pública sobre as **capacidades cibernéticas** nacionais também ajudaria a aumentar a transparência.[15] e, portanto, estabilidade e paz. Finalmente, à luz de todas as habilidades e conhecimentos necessários descritos abaixo, também é recomendado que os Estados desenvolvam **estratégias e planos nacionais para o desenvolvimento de habilidades cibernéticas**.

Estruturas e Processos

Os Estado-membros devem ter ou estabelecer estruturas múltiplas que aumentem a estabilidade e a segurança no uso das TIC, incluindo, no mínimo, **um centro nacional ou uma agência ou entidade responsável** que trate de todos os assuntos relacionados

14 Para obter orientações adicionais sobre como desenvolver estratégias nacionais de cibersegurança, consulte o Guia para o desenvolvimento de uma estratégia nacional de cibersegurança, produzido sob a coordenação da UIT com a participação de 18 parceiros de organizações internacionais, setor privado, sociedade civil e academia: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf.

15 Para o efeito, os Estados-membros podem fazer uso de plataformas relevantes como o Cyber Policy Portal, Cybil, a plataforma CoE Octopus, etc.

à cibersegurança; isso é fundamental para garantir a coordenação em nível nacional. A um nível mais operacional, as estruturas-chave adicionais que os Estados-membros devem ter disponíveis são: **capacidades nacionais ou regionais de deteção e resposta a ciberincidentes** (por exemplo, CERT/CSIRT ou Centros de Operações de Segurança), bem como **Pontos de Contacto (PoC)** a nível diplomático e técnico.[16] Os pontos de contacto podem desempenhar um papel fundamental na melhoria da comunicação entre os Estados-membros, contribuindo assim para a redução de potenciais crises em vários âmbitos e para gerar confiança.[17] Considerando a natureza criminosa de muitos incidentes cibernéticos, também deve ser considerada a **cooperação policial** (por exemplo, estabelecendo procedimentos para compartilhamento de informações). Para garantir que todas as medidas são tomadas em conformidade com o Marco, deve ser estabelecido um mecanismo de fiscalização (judicial, administrativo, parlamentar) independente e eficaz, capaz de garantir a transparência e a responsabilidade relativamente ao funcionamento do Estado no âmbito das TIC.

Associações e Redes

Como descreve o relatório do GEG de 2021, a cooperação abrangida por esta norma pode ser promovida em todos os níveis de governança. Para tanto, dois eixos principais de cooperação devem ser considerados: nacional e internacional. Por um lado, para reduzir os riscos de trabalhar em silos, seria essencial desenvolver a **cooperação intrassetorial** (por exemplo, com o setor privado, sociedade civil e academia) e **intragovernamental** (p. ex., reuniões interministeriais, grupos de trabalho). Por outro lado, é importante desenvolver a **cooperação a nível bilateral, regional e multilateral** em diferentes fases (p. ex., técnica, policial, diplomática) e recorrer a instrumentos já previstos em acordos multilaterais (p. ex., Convenção de Budapeste sobre o cibercrime ou a Convenção de Malabo para a proteção de dados pessoais).[18]

Pessoas e Habilidades

Tendo em vista a ampla gama de medidas que os Estado-membros podem adotar para implementar a Regra A, a tabela FCC identifica um conjunto amplo e básico de habilidades. Para os Estado-membros, as **capacidades diplomáticas** são importantes para participar de processos internacionais e intergovernamentais relacionados à segurança das TIC. À luz disso, também é benéfico para a equipe diplomática ter um **conhecimento básico de cibersegurança**. A fim de poderem participar adequadamente em fóruns internacionais, os Estados-membros também precisam de peritos jurídicos com **conhecimentos de direito internacional relativos a atividades**

16 Deve-se notar que, no momento da escrita, o estabelecimento de um diretório de PoCs nacionais foi amplamente discutido no contexto do OEWG. Espera-se que uma decisão formal sobre este ponto seja tomada durante a quinta sessão oficial do OEWG, agendada para 24 a 28 de julho de 2023. Embora as negociações em andamento se concentrem em um conselho PoC em nível estadual, também houve propostas e discutiu a possibilidade de desenvolver um diretório expandido que inclua outras partes interessadas.

17 Samuel Dominoni. 2023. Operationalizing a Directory of Points of Contact for Cyber Confidence-Building Measures. UNIDIR.

18 Este relatório reconhece as negociações em andamento do Comitê Ad Hoc para desenvolver uma convenção internacional abrangente para combater o uso criminoso de tecnologias de informação e comunicação.

no domínio das TIC. Por outro lado, quanto ao aspecto interno das medidas para aumentar a estabilidade e segurança no uso das TIC pelos Estados, é importante estabelecer programas de **treinamento de instrutores** com um vasto currículo sobre habilidades relacionadas à cibersegurança (isso também ajudaria a limitar as consequências da escassez global de habilidades em cibersegurança). Os Estados-membros também devem contar com **especialistas e investigadores em cibersegurança** capazes de acompanhar o cenário de ameaças em constante mudança. Por último, para efeitos da norma, também seria igualmente relevante a realização de **campanhas sistemáticas de conscientização** relacionadas à importância dos patches de segurança e outras práticas básicas de "ciberhigiene" voltadas ao público em geral.

Tecnologia

Embora a norma não determine o uso de tecnologias específicas, algumas tecnologias podem ser consideradas importantes para apoiar à implementação da norma. A tabela FCC identifica **recursos para garantir a proteção de produtos de TIC** (como antivírus e atualizações e patches automáticos em produtos digitais), **para prevenir, detectar e interromper atos maliciosos por meio de TIC** (como ferramentas de teste de penetração) e **para proteger as comunicações** (por exemplo, técnicas de criptografia).

3.2 Norma B

No caso de incidentes de TIC, os Estados devem considerar todas as informações relevantes, incluindo o contexto mais amplo do evento, as dificuldades de atribuição no ambiente das TIC e a natureza e extensão das consequências.

Políticas e Regulamentos

A atribuição é uma atividade complexa. Por esta razão, o desenvolvimento de uma **interpretação nacional** da norma é um elemento fundamental para a sua implementação. A interpretação abrangeria, por exemplo, que tipo(s) de atribuição (técnica, legal ou política)[19] está considerando o Estado e como ele os diferencia. Embora os Estados possam decidir fazer atribuições políticas com base apenas na atribuição técnica, recomenda-se que os Estado-membros publiquem **declarações (ou posições) sobre suas interpretações do direito internacional** sobre a responsabilidade do Estado no contexto das operações de TIC. Os Estados-membros devem então desenvolver e, idealmente, disponibilizar ao público **classificações de incidentes de TIC em termos de escala e impacto**. Isso ajudaria a aumentar a transparência sobre que tipo de incidentes maliciosos de TIC um Estado-membro interpretaria como um ato internacionalmente ilícito. É igualmente importante que os Estado-membros desenvolvam políticas que descrevam a **metodologia e cadeia de responsabilidade** do processo de atribuição; isso forneceria um marco útil e claro para a tomada de decisões relacionadas à atribuição e evitaria, por exemplo, cenários em que um Estado-membro realiza processos de atribuição paralelos por meio de diferentes órgãos estatais sem coordenação central. Em alguns casos, para proceder à atribuição, os Estados-membros podem necessitar de acesso a dados em poder por intervenientes não estatais. Portanto, recomenda-se a adoção de **regulamentos que estabeleçam os meios de compartilhamento de informações** entre atores governamentais e não governamentais.

Estruturas e Processos

Tendo em conta a dificuldade de identificar os responsáveis por um ato malicioso com as TIC e evitar o risco de atribuição errônea, uma vez que o ato malicioso tenha sido avaliado que o ato malicioso violou as disposições jurídicas ou regulamentares, os Estados-membros devem proceder à atribuição com base em **normas de prova adequados**.[20] Outro elemento importante para a implementação da norma diz respeito aos **processos e**

19 Ver Andraz Kastelic. 2021. Non-Escalatory Attribution of International Cyber Incidents Facts, International Law and Politics. UNIDIR.

20 Embora secundário ao objetivo deste estudo, deve-se observar que os normas de prova também podem ser relevantes para estabelecer a responsabilidade criminal individual e para processar o cibercrime de forma mais geral.

procedimentos que permitem o compartilhamento de informações com atores estatais e não estatais (inclusive para acesso a provas extraterritoriais), que podem ser cruciais para fazer atribuições fundamentadas.

Associações e Redes

Os atos maliciosos relacionados às TIC geralmente têm uma dimensão intersetorial/nacional. Portanto, para realizar a atribuição correta, recomenda-se a cooperação entre as partes interessadas nacionais e internacionais relevantes. Para o efeito, e ao nível da cooperação interna, seria útil a constituição de **grupos de trabalho ou plataformas que reúnam múltiplos interessados**. Isso aumentaria o compartilhamento de informações e reduziria o efeito do trabalho em silos. Em relação à cooperação internacional, é muito importante **promover a cooperação bilateral e multilateral em termos de assistência e compartilhamento de informações**. A cooperação a nível regional e internacional, incluindo cooperação entre Equipes de Resposta a Emergências de Informáticas (CERT), a Equipes de Resposta a Incidentes de Segurança de Informáticas (CSIRT) nacionais, as autoridades dos Estados responsáveis pelas TIC e a comunidade multissetorial podem fortalecer a capacidade dos Estados de detectarem e investigarem incidentes maliciosos relacionados com as TIC e fundamentarem suas preocupações e descobertas antes de chegar a uma conclusão sobre um incidente. Considerando os possíveis aspectos jurídicos derivados de uma atribuição, é importante estabelecer uma **cooperação bilateral e multilateral para a resolução de diferenças e controvérsias** por meio de consultas e outros meios pacíficos.

Pessoas e Habilidades

Fazer uma atribuição fundamentada pode envolver habilidades técnicas e legais. No que diz respeito aos primeiros, os Estados-membros devem dispor de **especialistas que efetuem a investigação técnica de incidentes TIC** (por exemplo, perícia forense TIC) ou, caso a investigação técnica seja efetuada por terceiros, **especialistas com capacidade para avaliar a sua qualidade**. No que diz respeito às competências jurídicas, os funcionários públicos (incluindo os funcionários diplomáticos) devem **ter conhecimento das disposições jurídicas** (a nível nacional e internacional) **específicas do contexto das TIC** e dos instrumentos disponíveis para resolver pacificamente os litígios sobre estas matérias, ou devem ser aconselhados por consultores em direito internacional sobre cibersegurança. Em casos de disputa, os funcionários públicos devem ser capacitados em **habilidades de negociação e comunicação** específicas para o contexto das TIC.

Tecnologia

Para apoiar as avaliações jurídicas e fornecer evidências úteis para sustentar decisões políticas relativas à atribuição, são necessários **recursos forenses e técnicos** para investigar e determinar a origem da atividade maliciosa relacionada com as TIC.

3.3 Norma C

Os Estados não devem permitir conscientemente que seu território seja usado para cometer atos internacionalmente ilícitos usando as TICs.

Políticas e Regulamentos

Recomenda-se que os Estados-membros desenvolvam as suas **interpretações nacionais da norma**, incluindo as suas opiniões sobre o conteúdo, âmbito e condições da norma (por exemplo, o que constitui um ato internacionalmente ilícito utilizando as TIC). No que diz respeito à aplicação da norma, e considerando a expectativa de que, se um Estado tiver conhecimento, ou for notificado de boa-fé, que um ato internacionalmente ilícito que utilize as TIC tenha origem em seu território, "tomará as medidas razoáveis dentro de suas possibilidades pôr termo à atividade em curso no seu território".[21] Os Estados-membros devem ter uma **estratégia ou política de cibersegurança** que estabeleça as disposições que lhes permitam agir (por exemplo, detectar e interromper) em caso de incidente malicioso com recurso às TIC. Além disso, os Estados também devem elaborar **legislação** que defina quais tipos de atividades de TIC são e quais não são permitidos no território do Estado e que conceda autoridade para investigar, encerrar e processar esses tipos de atividades.

Estruturas e Processos

São necessárias estruturas e processos apropriados que permitam a um Estado agir quando toma conhecimento ou é notificado de boa fé de que um ato internacional ilícito se origina em seu território. Para esse fim, **ter capacidade nacional ou regional de detecção e resposta a incidentes cibernéticos** (por exemplo, um CERT/CSIRT ou Centro de Operações de Segurança) e **recursos de aplicação da lei cibernética** (por exemplo, uma unidade de crimes cibernéticos nas forças policiais) ou uma agência equivalente com poder para investigar e processar, ajudaria os Estado-membros a lidar com as ameaças por meio de meios proporcionais, apropriados e eficazes de acordo com o direito internacional e nacional. Além disso, considerando a natureza dos incidentes maliciosos de TIC, deveriam ser estabelecidos **procedimentos para compartilhar informações** entre as partes interessadas nacionais relevantes (por exemplo, memorandos de entendimento delineando a cooperação entre a aplicação da lei e os provedores de serviços de Internet). A regra também destaca a necessidade de solicitar ajuda de outros Estados-membros. Neste caso é importante **estabelecer mecanismos de envio ou resposta a pedidos de assistência** (incluindo um PoC ou entidade nacional designada para receber pedidos de assistência e procedimentos para avaliar a adequação desses pedidos).

21 GGE. 2021, para. 30(a).

Associações e Redes

O estabelecimento de procedimentos para a compartilhamento de informações tanto a nível nacional como internacional exige que os Estado-membros criem mecanismos de cooperação. No nível nacional, isto pode ser feito através da criação **de grupos de trabalho conjuntos, plataformas de múltiplos interessados** (com atores estatais e não estatais, incluindo CERTs/CSIRTs nacionais) e/ou **parcerias público-privadas** em setores-chave. A nível internacional, pode incluir **acordos bilaterais ou multilaterais para assistência e compartilhamento de informações** (p. ex., assistência jurídica mútua). Recomenda-se também a adesão aos **marcos de compartilhamento de informações existentes no nível técnico** (por exemplo, a rede FIRST), que reúnem uma vasta gama de conhecimentos técnicos e possibilidades de cooperação a nível mundial.

Pessoas e Habilidades

A norma refere-se às providências razoáveis que um Estado deve adotar para pôr fim às atividades maliciosas. Por conseguinte, os Estados-membros devem ter acesso a **conhecimentos técnicos especializados em cibersegurança**, internos ou externos, que lhes permitam identificar e interromper atos maliciosos das TIC alocados no seu território (p. ex., competências em matéria de segurança de redes). Outro conjunto relevante de competências diz respeito às **comunicações específicas no contexto das TIC** que seriam necessárias para gerir a comunicação pública e confidencial após um incidente; isso inclui **pessoal diplomático**.

Tecnologia

As capacidades tecnológicas relacionadas com esta norma dizem respeito à **identificação, deteção e interrupção de atos maliciosos que utilizam as TIC** alocados no território dos Estado-membros.

3.4 Norma D

Os Estados devem considerar a melhor forma de cooperar para trocar informações, prestarem assistência mútua, processar judicialmente o uso terrorista e criminoso das TIC e aplicar outras medidas de cooperação para lidar com esse tipo de ameaça. Os Estados poderão ter de considerar a necessidade de desenvolver novas medidas a esse respeito.

Políticas e Regulamentos

Esta norma refere-se a conceitos ainda abertos à interpretação (por exemplo, o uso de TIC por terroristas). Por esta razão, uma capacidade relevante e essencial é publicar uma **interpretação nacional da norma** na qual os Estado-membros desenvolvam seus pontos de vista. Recomenda-se também a **assinatura e ratificação de instrumentos bilaterais, regionais ou multilaterais** sobre crimes cibernéticos.[22] Esses instrumentos facilitam a cooperação oportuna e eficaz entre os Estados. Além disso, devido à perspectiva operacional da norma, é importante que os Estado-membros adotem **políticas que descrevam os mecanismos ou procedimentos de cooperação**, especialmente para **o compartilhamento de informações**, inclusive com o setor privado (p. ex., por meio do código penal). Para melhor cooperar nesses campos, recomenda-se a elaboração de **legislação sobre crimes cibernéticos** que assegure uma abordagem tecnologicamente neutra.[23]

Estruturas e Processos

Nesta norma, é muito importante estabelecer **mecanismos eficientes de envio e resposta a solicitações de assistência** (p. ex., solicitação de assistência jurídica mútua). Igualmente importante é desenvolver corretamente **protocolos e procedimentos** que permitam o uso de provas digitais em tribunal. Esses protocolos e procedimentos devem especificar diretrizes para a coleta, manuseio e armazenamento adequados de evidências digitais. É também importante que os Estados-membros desenvolvam e reforcem a sua **capacidade de aplicação da lei cibernética** (por exemplo, unidades ciberpoliciais), para que possam cooperar eficazmente a nível operacional no combate à utilização criminosa e terrorista das TIC. Além disso, ter **capacidade nacional ou regional para detectar e responder a incidentes cibernéticos** (p. ex., CERT/CSIRT ou Centros de Operações de Segurança) é fundamental para identificar, documentar e comunicar atos maliciosos que utilizem as TIC.

---

22 Embora a definição de cibercrime possa variar em diferentes legislações nacionais, para efeitos deste estudo definimo-lo como crimes contra a integridade, disponibilidade e confidencialidade dos dados.

23 A adoção de uma abordagem tecnologicamente neutra ao redigir novos projetos de lei ou emendas legais relacionadas às TIC agrega flexibilidade ao envio e recebimento de solicitações e permite que você acompanhe a velocidade dos desenvolvimentos tecnológicos; ver Samuele Dominioni, 2021 Enhancing Cooperation to Address Criminal and Terrorist Use of ICTs Operationalizing Norms of Responsible State Behaviour in Cyberspace. UNIDIR.

Associações e Redes

A norma está centrada na cooperação, que pode ocorrer em vários níveis. Os Estado--membros devem estabelecer ou fortalecer **mecanismos bilaterais, regionais e multilaterais para cooperar** na investigação e processamento judicial do cibercrime. Neste contexto, os tratados de assistência jurídica mútua continuam a prevalecer. Também são essenciais **redes operacionais e técnicas** entre, por exemplo, aplicação da lei (por exemplo, INTERPOL I-24/7) e serviços de resposta a incidentes (por exemplo, FIRST), através dos quais os agentes podem ter acesso rápido a recursos relevantes (por exemplo, bancos de dados). Finalmente, **a cooperação entre as partes interessadas nacionais**, incluindo o setor privado (por exemplo, parcerias público-privadas), é importante para evitar o trabalho isolado e, assim, promover uma cooperação mais eficaz e coordenada com outros Estados-membros.

Pessoas e Habilidades

A fim de implementar adequadamente a norma, os Estados-membros devem formar o seu pessoal em diferentes competências.[24] Recomenda-se ter **especialistas na manipulação de evidências digitais a nível técnico e jurídico**. Também é importante a capacitação na redação de pedidos de auxílio jurídico mútuo, no uso de outras ferramentas (como mandados de busca específicos para evidências digitais) ou o armazenamento e compartilhamento adequados de dados durante as investigações de crimes cibernéticos. Caso contrário, os tribunais podem não autorizar ou aceitar a apreensão de evidências digitais. Os Estados-membros também devem dispor de pessoal que tenha **conhecimento da legislação relativa à cibercrimes nos outros Estados-membros**.[25] Finalmente, para melhorar a cooperação entre as partes interessadas, é importante que o pessoal dos Estados-membros (por exemplo, pessoal diplomático) tenha a **capacidade de se conectar (mesmo informalmente) com os seus pares bilaterais, regionais e internacionais** e outros parceiros, a fim de garantir que as intervenções sejam eficientes e oportunas.

Tecnologia

A tecnologia necessária para a implementação da norma é dividida em duas áreas principais. Por um lado, existem capacidades tecnológicas para **prevenir, detectar ou interromper atos maliciosos com TIC** (por exemplo, plataformas de inteligência de ameaças).[26] Por outro lado, existem as capacidades relacionadas a **canais de comunicação seguros** ou plataformas de compartilhamento de informações (por exemplo, software de compartilhamento de dados policiais).

---

24 Nesse contexto, vale destacar o Programa Global sobre Crimes Cibernéticos liderado pelo UNODC: **Global Programme on Cybercrime (unodc.org)**.

25 Isso é especialmente importante para os Estado-membros que precisam enviar um pedido de assistência a outro Estado; ver Samuele Dominioni, 2021 Enhancing Cooperation to Address Criminal and Terrorist Use of ICTs Operationalizing Norms of Responsible State Behaviour in Cyberspace. UNIDIR.

26 Uma Plataforma de Inteligência de Ameaças (TIP) é "uma solução de tecnologia que coleta, agrega e organiza dados de inteligência de ameaças de várias fontes e em vários formatos"; veja: múltiplas fontes e formatos"; ver: **https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform#:~:text=A%20Threat%20Intelligence%20Platform%20(TIP,threat%20identification%2C%20investigation%20and %20resposta**.

3.4 Norma E

Os Estados, ao garantir o uso seguro das TIC, devem respeitar as resoluções 20/8 e 26/13 do Conselho de Direitos Humanos relacionadas à promoção, proteção e gozo dos direitos humanos na Internet, bem como as resoluções 68/167 e 69/166 da Assembleia Geral sobre o direito à privacidade na era digital, a fim de garantir o pleno respeito aos direitos humanos, incluindo o direito à liberdade de expressão.

Políticas e Regulamentos

Esta é uma das regras gerais que abrange todos os recursos de todos os componentes da norma. Consequentemente, para assegurar a coerência da sua aplicação, os Estados-membros devem publicar uma **posição nacional sobre a forma como o direito internacional, incluindo o direito internacional dos direitos humanos, no âmbito das TIC**. Portanto, é essencial que os Estado-membros **desenvolvam políticas e estratégias de cibersegurança consistentes com a lei internacional de direitos humanos** (por exemplo, orientação nas resoluções 68/167 e 69/166). A norma também prevê a não imposição de restrições indevidas à liberdade de expressão e à liberdade de buscar, receber e divulgar informações. Na maioria dos casos, isto seria implementado **abstendo-se de tais restrições** (por exemplo, g., através da censura de sites). Em vez disso, os Estados-membros devem **adotar regulamentos, inclusive para empresas, relativos ao respeito pelos direitos humanos na concepção, desenvolvimento e uso de novas tecnologias**. Além disso, recomenda-se a adoção de **legislação que estabeleça limites à vigilância e interceptação pelo Estado**, de acordo com o direito à privacidade. Por último, os Estados-membros devem ter **leis de proteção de dados** que definam o marco jurídico para o tratamento de dados de pessoas físicas.

Estruturas e Processos

Os Estados-membros devem criar **mecanismos de supervisão nacionais ou regionais independentes e eficazes** (por exemplo, judiciais, administrativos ou parlamentares) capazes de assegurar a transparência, proporcionalidade e prestação de contas em relação à vigilância das comunicações, intercepção e coleta de dados pessoais. Estes mecanismos podem referir-se a entidades específicas (ad hoc) ou a entidades já existentes com autoridade específica para garantir os princípios acima referidos (por exemplo, uma comissão parlamentar).

Associações e Redes

As camadas adicionais de entendimento no relatório do GEG 2021 reconhecem que "várias partes interessadas podem contribuir de diferentes maneiras para a proteção

e promoção dos direitos humanos e liberdades fundamentais on-line e off-line".[27] Diante disso, seria essencial **participar e consultar as partes interessadas** que defendem, promovem e analisam (por exemplo, a academia) os direitos humanos e as liberdades fundamentais online para entender e minimizar os potenciais impactos negativos dessas políticas nas pessoas.

Pessoas e Habilidades

Considerando o objetivo geral da norma e suas implicações específicas, é pertinente que os funcionários públicos (incluindo aqueles que trabalham na aplicação da lei) tenham **conhecimento dos direitos humanos na esfera digital**,[28] bem como **sobre a forma de implementar instrumentos internacionais** (por exemplo, pedidos de assistência jurídica mútua) de forma **coerente com os direitos humanos**. Por outro lado, é importante que os Estado-membros tenham **especialistas em direitos humanos** com conhecimentos especializados em seus contextos específicos.

Tecnologia

Existem algumas **capacidades tecnológicas para garantir o respeito aos direitos humanos** no uso das TICs por atores estatais e não estatais. Em particular, as soluções de cibersegurança de pontos finais *"endpoint"* podem proteger contra spyware e o software de criptografia pode proteger as comunicações.

27 GGE. 2021, para. 41.

28 Existem cursos disponíveis, como um curso do Conselho da Europa sobre educação em direitos humanos para profissionais do direito que se concentra em crimes cibernéticos e evidências eletrônicas; ver: https://www.coe.int/en/web/help/courses#{%2258133235%22:[9]}.

3.6 Norma F

Um Estado não deve conduzir ou apoiar conscientemente uma atividade de TIC contrária às suas obrigações ao abrigo do direito internacional que danifique intencionalmente a infraestrutura crítica ou prejudique de qualquer outra forma o uso e a operação de infraestrutura crítica necessária para prestar serviços ao público.

Políticas e Regulamentos

Tendo em conta o enfoque da norma nas obrigações dos Estados ao abrigo do direito internacional, recomenda-se que os Estado--membros desenvolvam e disponibilizem ao público suas **posições nacionais sobre como o direito internacional** se aplica ao uso das TICs pelos Estados. É importante que eles apresentem suas **interpretações nacionais** do termo "apoio consciente", suas **classificações de incidentes de TIC** em termos de escala e gravidade (inclusive com referência ao que se entende por "dano" e "prejuízo") e seu **conceito do que constitui, em seu contexto nacional, "infraestrutura crítica**".[29] Isto permite que os Estados-membros especifiquem quais as infraestruturas ou setores conexos que consideram críticos.

Estruturas e Processos

Para garantir que o objetivo da norma seja cumprido, os Estados-membros devem estabelecer **mecanismos de supervisão nacionais ou regionais que sejam independentes, eficazes** (judiciais, administrativos, parlamentares) e capazes de garantir a transparência no comportamento dos Estados (por exemplo, uma comissão parlamentar).

Associações e Redes

Dada a dimensão transnacional da atuação dos Estados no âmbito das TIC, seria fundamental que os Estado-membros participassem de **marcos de cooperação bilateral, regional e multilateral** para o compartilhamento de informações, inclusive no que diz respeito à interpretação nacional da norma. Isto poderia contribuir para aumentar a transparência em torno de suas designações de infraestrutura crítica e dos seus métodos de categorização, a fim de ajudar a construir entendimentos comuns sobre a proteção de setores considerados críticos.

Pessoas e Habilidades

Os funcionários públicos devem ter **conhecimento jurídico, incluindo direito**

29 Por exemplo, saúde, energia, geração de energia, água e saneamento, educação, negócios e serviços financeiros, transporte, telecomunicações e processos eleitorais e a infraestrutura essencial para a disponibilidade e integridade geral da Internet; ver OEWG, 2021. Final Substantive Report, par. 18.

internacional e sua aplicabilidade no domínio das TIC, para implementar a norma e suas capacidades fundamentais relacionadas (por exemplo, interpretação nacional da norma).

Tecnologia

Este estudo não identificou nenhuma capacidade tecnológica crítica necessária para implementar esta norma.

3.7 Norma G

Os Estados devem tomar as medidas apropriadas para proteger sua infraestrutura crítica contra ameaças relacionadas às TIC, levando em consideração a resolução 58/199 da Assembleia Geral.

Políticas e Regulamentos

Em primeiro lugar, seria importante que os Estados-membros elaborassem a sua interpretação nacional da norma e, nessa interpretação, definissem o seu entendimento do termo "apropriado". Este documento deve também incluir quais **setores de infraestrutura crítica** consideram que devem ser protegidos, bem como as **classificações de incidentes de TIC, em termos de escala e gravidade**, específicas para suas infraestruturas críticas.[30] A fim de proteger as infraestruturas críticas, é essencial que os Estados-membros adotem um marco legislativo adequado para o efeito (por exemplo, estabelecendo regulamentos sobre a sua construção, incluindo normas mínimas de segurança, mecanismos de notificação e auditorias). Por outro lado, conforme estabelecido na norma, os Estado-membros devem **considerar**, em suas políticas e estratégias de cibersegurança, **a resolução 58/199 da Assembleia Geral**[31] na redução de riscos para infraestruturas de informação críticas. Finalmente, dado que em muitos países os atores não estatais desempenham um papel importante na gestão das infraestruturas críticas, seria importante estabelecer **regulamentos sobre o compartilhamento de informações entre os setores público e privado.**

Estruturas e Processos

Em termos de estruturas, os Estados-membros devem criar **um centro ou agência nacional responsável por infraestruturas críticas**, bem como capacidades nacionais ou regionais de deteção e resposta a ciberincidentes (por exemplo, CERT/CSIRT ou Centros de Operações de Segurança) que desempenhem um papel fundamental na proteção de infraestruturas críticas. Em termos de processos, é importante que os Estados-membros estabeleçam e implementem **mecanismos concebidos para garantir o cumprimento** das normas relevantes e outros requisitos regulamentares (por exemplo, auditorias, testes de preparação e exercícios baseados em cenários para testar a resiliência e eficácia dos mecanismos e procedimentos de resposta a incidentes); também **planos de contingência** em caso de incidentes com as TIC que afetem infraestruturas críticas (incluindo medidas para restaurar a funcionalidade de infraestruturas críticas danificadas). Finalmente,

30 Os dois documentos podem ser emitidos separadamente.

31 Esta resolução, intitulada "Criação de uma cultura global de cibersegurança e proteção de infraestruturas críticas de informação", estabelece 11 elementos para a proteção de infraestruturas críticas de informação. A resolução também convida os Estado-membros a levarem em consideração esses 11 elementos ao desenvolverem suas estratégias de redução de riscos para infraestruturas críticas de informação, de acordo com as leis e regulamentações nacionais. Para mais informações, veja: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf?OpenElement.

é necessário implementar **processos e procedimentos que permitam o compartilhamento de informações** entre entidades governamentais e não governamentais envolvidas no ecossistema das infraestruturas críticas.

Associações e Redes

Dada a dimensão transnacional de muitos dos incidentes que envolvem as TIC e algumas infraestruturas críticas, recomenda-se que os Estados-membros estabeleçam uma **cooperação transfronteiriça com as partes interessadas relevantes** (por exemplo, operadores e proprietários) para partilhar informações e boas práticas de proteção de infraestruturas críticas e coordenar as respostas. Isto pode incluir a participação dos Estados em iniciativas voluntárias de avaliação de risco e planejamento de continuidade de negócios (resiliência, recuperação e contingência) com a participação de outras partes interessadas, que visam melhorar a segurança e resiliência das infraestruturas críticas que prestam serviços a nível regional ou internacional contra ameaças existentes ou emergentes. Além disso, tendo em conta o ecossistema multifacetado das infraestruturas críticas, e a fim de assegurar uma proteção coerente e abrangente, os Estados-membros **devem estabelecer mecanismos de cooperação entre as partes interessadas nacionais pertinentes** (por exemplo, comités interserviços, plataformas multilaterais), incluindo parcerias público-privadas com proprietários, operadores ou gestores de infraestruturas críticas.

Pessoas e Habilidades

Existem várias habilidades que os Estado-membros precisam ter em conta ao implementar esta norma. Por um lado, **habilidades técnicas** para melhorar a cibersegurança de infraestruturas críticas e a resposta e gestão de incidentes de TIC (por exemplo, segurança de redes, análise forense digital etc.). Por outro lado, os Estados-membros **devem realizar** treinamentos e exercícios que testem a continuidade do serviço e os planos de contingência para incidentes que afetem as infraestruturas críticas e devem incentivar os interessados a participar de atividades semelhantes. Finalmente, o pessoal diplomático deve ter as competências necessárias para **interagir com os seus homólogos na questão específica das infraestruturas críticas**, especialmente se estas forem transnacionais.

Tecnologia

Em termos de tecnologia, recomenda-se que os Estados-membros tenham **capacidade técnica para prevenir, detectar e interromper atos maliciosos de TIC direcionados para infraestruturas críticas**. Estes podem incluir, entre outros, plataformas de inteligência de ameaças,[32] sistemas de alerta precoce,[33] ferramentas de rastreio de vulnerabilidade[34] e perímetros seguros.[35]

---

32 Uma plataforma de inteligência de ameaças automatiza a coleta, agregação e reconciliação de dados de ameaças externas; ver: **https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-platforms/#:~:text=A%20threat%20intelligence%20platform%20automatiza,risks%20relevant%20for%20their%20organization)**.

33 Um sistema de alerta antecipado é um serviço de notificação de ameaças que relata atividades potencialmente suspeitas na rede; ver: **https://www.ncsc.gov.uk/blog-post/early-warning-whats-new-and-whats-in-it-for-you**.

34 Eles são ferramentas automatizadas para descobrir, analisar e relatar falhas e vulnerabilidades de segurança em uma rede.

35 Por exemplo, através da implementação de soluções com isolamento físico (air-gapped: sem ligação entre redes locais e externas) ou com a utilização de firewalls.

3.8 Norma H

Os Estados devem responder às solicitações apropriadas de assistência de outro Estado cuja infraestrutura crítica esteja sujeita a atos maliciosos de TIC. Os Estados também devem responder às solicitações apropriadas para mitigar atividades maliciosas relacionadas às TIC direcionadas à infraestrutura crítica de outro Estado e originárias de seu território, com o devido respeito por sua soberania.

Políticas e Regulamentos

O texto desta norma contém vários conceitos e responsabilidades que os Estado-membros precisam esclarecer. Portanto, uma **interpretação nacional desta norma** ajudaria os Estado-membros a esclarecer o que eles querem dizer com, por exemplo, "solicitações apropriadas" ou "infraestrutura crítica" (ver também Norma G). É importante que os Estado-membros adotem posteriormente legislação que forneça um **marco para solicitar e fornecer assistência internacional e estratégias e políticas de cibersegurança** que detalhem os mecanismos, procedimentos e processos para iniciar, enviar e responder a pedidos de assistência.

Estruturas e Processos

Dada a perspectiva transnacional e de cooperação da norma, os Estados-membros devem criar **mecanismos eficazes para receber, processar, avaliar e responder aos pedidos de assistência, bem como para os preparar e enviar**.[36] Além disso, tendo em conta a dimensão coercitiva da norma, que obriga os Estados-membros a mitigar as atividades maliciosas das TIC alocados no seu território, recomenda-se que os Estados-membros estabeleçam as capacidades necessárias para a aplicação do direito cibernético.

Associações e Redes

A nível internacional, os Estados-membros devem aderir a **instrumentos ou acordos de cooperação bilateral, regional e multilateral para a proteção de infraestruturas críticas**. Estas redes podem ajudar a gerir os pedidos de assistência (por exemplo, podem ter modelos comuns disponíveis ou mecanismos específicos para comunicação de crises ou gestão de incidentes que os Estados-membros podem ativar). Além disso, dado o papel que os atores não estatais (muitas vezes internacionais) desempenham na gestão de infraestruturas críticas, é importante estabelecer **cooperação transfronteiriça com proprietários e operadores de infraestruturas**

36 Los mecanismos eficientes para recibir y enviar solicitudes de información pueden incluir la creación de plantillas o documentos orientadores sobre qué información se incluirá en las solicitudes, el establecimiento de puntos de contacto para asuntos técnicos y un comité ad hoc u otra entidad para evaluar la idoneidad de um pedido.

importantes, bem como com provedores (por exemplo, coordenação de sistemas de alerta de emergência e compartilhamento e análise de informações sobre vulnerabilidades). A nível nacional, recomenda-se a promoção da cooperação entre os interessados relevantes para a proteção das infraestruturas críticas (por exemplo, parcerias público-privadas e comités interinstitucionais). Estas disposições contribuiriam para aumentar o compartilhamento de informações e para realizar intervenções oportunas e eficazes.

Pessoas e Habilidades

Para implementar esta norma, os Estados-membros devem ter **pessoal formado para gerir a assistência transfronteiriça na proteção de infraestruturas críticas** (por exemplo, investigadores de cibersegurança, especialistas em gestão de riscos da cadeia de abastecimento e de resposta a incidentes). Por outro lado, uma solicitação de assistência pode se referir a vários aspectos da proteção de infraestrutura crítica; portanto, a equipe que recebe ou envia solicitações de assistência deve ter uma noção clara de **como atender e gerenciar uma solicitação de assistência.**

Tecnologia

Em termos de tecnologia, é importante que os Estados-membros desenvolvam as **capacidades necessárias para prevenir, detectar e interromper atos maliciosos de TIC direcionados para infraestruturas críticas**. Estes podem incluir, entre outros, plataformas de inteligência de ameaças,[37] sistemas de alerta precoce[38] e ferramentas de rastreio de vulnerabilidade.[39] Adicionalmente, como a norma se centra na assistência, os Estados-membros devem estabelecer **canais de comunicação ou plataformas seguras** para o compartilhamento de informações relacionadas com atos maliciosos contra infraestruturas críticas.

37 Uma plataforma de inteligência de ameaças automatiza a coleta, agregação e reconciliação de dados de ameaças externas; ver: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligenceplatforms/#:~:text=A%20threat%20intelligence%20platform%20automatiza,risks%20relevant%20for%20their%20organization).

38 Um sistema de alerta antecipado é um serviço de notificação de ameaças que relata atividades potencialmente suspeitas na rede; ver: https://www.ncsc.gov.uk/blog-post/early-warning-whats-new-and-whats-in-it-for-you.

39 Eles são ferramentas automatizadas para descobrir, analisar e relatar falhas e vulnerabilidades de segurança em uma rede.

3.9 Norma I

Os Estados devem tomar medidas razoáveis para garantir a integridade da cadeia de abastecimento para que os usuários finais possam confiar na segurança dos produtos de TIC. Os Estados devem tentar impedir a proliferação de ferramentas e técnicas de TIC maliciosas e o uso de funções ocultas nocivas.

Políticas e Regulamentos

Dada a complexidade e a estrutura multifacetada das cadeias de abastecimento contemporâneas, é importante que os Estados-membros definam a sua **interpretação nacional da norma** (por exemplo, especificando o que entendem por "medidas razoáveis"). Recomenda-se também que os Estados-membros promulguem **legislação que proíba a introdução de funções ocultas prejudiciais e a exploração de vulnerabilidades em produtos de TIC**.[40] Esta legislação constituiria a base legal para prevenir (e processar juridicamente) atos maliciosos contra a cadeia de abastecimentos. Além disso, é importante que os Estados-membros adotem uma **política ou estratégia de cibersegurança que abranja a segurança da cadeia de abastecimento**, descrevendo eventualmente um marco para a gestão dos riscos da cadeia de abastecimento com base numa avaliação de riscos que considere uma série de fatores, incluindo os benefícios e riscos de novas tecnologias.

Finalmente, a fim de evitar o surgimento de estruturas múltiplas e diferentes para a regulamentação da segurança da cadeia de abastecimento, recomenda-se que os Estado-membros estabeleçam os **requisitos para implementar regras e padrões comuns globalmente interoperáveis para a segurança da cadeia de abastecimento**. (por exemplo, ISO/IEC 20243). Tendo em conta todos os aspectos de segurança envolvidos na produção de produtos TIC, os Estados-membros devem instar que os provedores **incluam segurança e proteção na gestão do ciclo de vida dos seus produtos.**

Estruturas e Processos

Para a aplicação esta norma, os Estado-membros devem implementar **mecanismos de governança para gestão de riscos na cadeia de abastecimento**, que devem incluir os atores-chave que representam os nós da cadeia de valor. Isto é especialmente importante porque permitiria aos Estados-membros identificar,

40 Alguns exemplos adicionais de possíveis intervenções legislativas são: medidas para impedir a adulteração de produtos e serviços durante o desenvolvimento e a produção, se isso puder prejudicar substancialmente a estabilidade do ciberespaço e medidas para proibir qualquer pessoa dentro de seu território ou jurisdição de participar de operações cibernéticas que possam comprometer a segurança, integridade ou confidencialidade dos produtos e serviços comerciais de TIC.

monitorizar e avaliar os riscos na cadeia de abastecimento.[41] Além disso, em termos de estrutura, recomenda-se que os Estado-membros introduzam um **mecanismo de avaliação e certificação**, quer através da criação de uma entidade nacional específica, quer através de parcerias com outros Estados que já tenham esta capacidade. Por último, os Estados-membros devem **garantir a interoperabilidade** (entre jurisdições) de abordagens, métodos de certificação e certificações dos produtos TIC.

Associações e Redes

Dadas as dimensões transnacionais da maioria das cadeias de abastecimento, os Estados-membros devem desenvolver **medidas de cooperação bilateral, regional e multilateral** para, por exemplo, compartilhamento de boas práticas de gestão dos riscos da cadeia de abastecimento ou certificação de produtos TIC, e compartilhamento de informações sobre vulnerabilidades relacionadas às TIC ou funções ocultas prejudiciais em produtos.

Pessoas e Habilidades

Existem vários conjuntos de habilidades que os Estado-membros precisam considerar ao implementar esta norma. Em primeiro lugar, **competências técnicas e organizacionais** para gerir a segurança das cadeias de abastecimento. Estas incluem, entre outras, habilidades para identificar, monitorar e intervir para resolver vulnerabilidades da cadeia de abastecimento e avaliar sua resiliência. Então, **diante** de atos maliciosos com TIC, as **habilidades de resposta a incidentes e de gestão** também são essenciais. Por último, dada a importância das cadeias de abastecimento para a segurança internacional, é relevante que o pessoal diplomático dos Estados-membros **seja capaz de interagir significativamente** com os seus homólogos no que diz respeito ao **tema específico da segurança da cadeia de abastecimento**.

Tecnologia

É importante que os Estados-membros tenham **capacidade técnica para prevenir, detectar ou interromper os ataques às cadeias de abastecimento**. Estas capacidades podem incluir, entre outras, plataformas de inteligência de ameaças e[42] sistemas de alerta precoce.[43] Os Estado-membros (caso desejem avaliar os produtos de TIC) também devem ter ferramentas disponíveis para obtenção e análise de código (code sourcing e code fuzzing).[44]

---

41 Para o efeito, os Estados-membros podem obrigar os provedores a utilizar as chamadas listas de materiais de software (SBOM, que são inventários que listam todos os componentes de software), uma vez que tal permitiria aos Estados-membros avaliar rapidamente se existe um risco para a cadeia de abastecimento no primeiro lugar.

42 Uma plataforma de inteligência de ameaças automatiza a coleta, agregação e reconciliação de dados de ameaças externas; ver: **https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-platforms/#:~:text=A%20threat%20intelligence%20platform%20automatiza,risks%20relevant%20for%20their%20organization)**.

43 Um sistema de alerta antecipado é um serviço de notificação de ameaças que relata atividades potencialmente suspeitas na rede; ver: **https://www.ncsc.gov.uk/blog-post/early-warning-whats-new-and-whats-in-it-for-you**.

44 *Code souring* y *fuzzing* são dois métodos de localização e tratamento de vulnerabilidades no código de software.

3.10 Norma J

Os Estados devem encorajar o relato responsável de vulnerabilidades de TIC e compartilhar as informações correspondentes sobre soluções disponíveis para tais vulnerabilidades, a fim de limitar e possivelmente eliminar ameaças potenciais às TIC e à infraestrutura dependente de TIC.

Políticas e Regulamentos

Para implementar **adequadamente a norma, é muito importante que os Estado-membros desenvolvam sua interpretação** nacional da norma, e isso inclui, por exemplo, como eles interpretam "notificação responsável" e "compartilhamento de informações [...] soluções disponíveis". Do ponto de vista legislativo, é fundamental que os Estados-membros tomem posteriormente **medidas legais para impedir a distribuição comercial de vulnerabilidades** (por exemplo, estabelecendo limites estritos para o desenvolvimento, armazenamento e venda de vulnerabilidades de TIC por atores do setor privado para fins de ganho financeiro) e para **descriminalizar e proteger os pesquisadores de cibersegurança e** *hackers* **éticos** que desejam identificar vulnerabilidades. É igualmente importante **estabelecer uma política de divulgação de vulnerabilidade coordenada (CVD)** (que pode ser incluída na estratégia ou política de cibersegurança ou adotada como um instrumento autônomo) com base na suposição de divulgação privada sobre contenção de vulnerabilidade.[45] Para compartilhar informações sobre novas vulnerabilidades e soluções disponíveis, também é recomendável implementar **estruturas legais que permitam a cooperação e a compartilhamento de informações com vendedores e provedores**. Em relação aos provedores e provedores, é pertinente que os Estado-membros estabeleçam com precisão os **requisitos necessários para que as políticas e práticas de gerenciamento de vulnerabilidades sejam eficientes e eficazes** de modo a minimizar os potenciais efeitos adversos de produtos vulneráveis e sistematizar a comunicação das vulnerabilidades das TIC.

Estruturas e Processos

Os Estados-membros devem criar os processos e estruturas necessários para o bom funcionamento da política coordenada de

45 Entendemos que alguns Estados, em determinadas circunstâncias, podem preferir não divulgar vulnerabilidades. Nesses casos, recomendamos o desenvolvimento de uma política de ações frente as vulnerabilidades (*vulnerability equities policy*) que permita aos Estado-membros avaliar caso a caso se devem disseminar informações sobre vulnerabilidade ou restringi-las temporariamente para fins de segurança nacional ou aplicação da lei.

46 Existem bons recursos de domínio público para apoiar os Estados na concepção de seus aparatos nacionais de DCV; veja por exemplo **https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCVD+2022_04/about**.

divulgação de vulnerabilidades.[46] Como indica o relatório GEG 2021, isso deve incluir **orientações sobre as respectivas funções e responsabilidades** de diferentes partes interessadas nos processos de divulgação, os tipos de informações técnicas a serem divulgadas ou compartilhadas publicamente e o tratamento de dados confidenciais para garantir a segurança e a confidencialidade das informações . Além disso, os Estado-membros devem criar **protocolos para comunicação e compartilhamento de informações entre todas as partes interessadas relevantes** (por exemplo, governos, provedores e vendedores, investigadores de segurança e equipes de resposta a incidentes) e para **compartilhamento de atualizações e sistemas de correção**. É importante que eles implementem incentivos subsequentes (por exemplo, programas de recompensa por erros) e, como indica o relatório do GEG de 2021,[47] Por último, seria fundamental a implementação de **campanhas sistemáticas de sensibilização** (tanto dirigidas ao público em geral como ao pessoal de setores específicos) sobre a importância dos patches de segurança.

Associações e Redes

Levando em conta as dimensões intersetoriais e transnacionais da divulgação responsável da vulnerabilidade, é apropriado desenvolver a **cooperação bilateral, regional e multilateral** nessa área. Na verdade, o relatório do GEG de 2021 menciona a cooperação internacional como um elemento fundamental de "um processo confiável e coerente para divulgações de rotina".[48] O **estabelecimento de cooperação intersetorial** com o setor privado, a sociedade civil e a comunidade técnica, incluindo provedores e proprietários, é igualmente importante.

Pessoas e Habilidades

Existem três conjuntos diferentes de habilidades que são importantes para a implementação desta norma. Primeiro, **habilidades técnicas**, incluindo habilidades para identificar e resolver vulnerabilidades ou gerenciar informações relacionadas a vulnerabilidades (por exemplo, informações fornecidas por empresas que oferecem recompensas por erros, pesquisadores de segurança e provedores). Em segundo lugar, as **habilidades de comunicação pública** também são relevantes, especialmente quando é vital abordar o público em geral sobre as vulnerabilidades que afetam a população. Finalmente, tendo em vista o potencial impacto das vulnerabilidades na segurança internacional, são necessárias **habilidades diplomáticas e de comunicação** para participar com êxito em debates sobre a gestão da vulnerabilidade com os Estados e os interessados não estatais relevantes.

---

47 Os governos que desejam manter a possibilidade de contenção e não divulgação devem desenvolver um processo específico, descrito em um documento público, para gerenciar quando e como um governo escolherá divulgar as vulnerabilidades cibernéticas que descobrir ou adquirir. Esse processo deve incluir, por exemplo, um comitê de avaliação de vulnerabilidade entre agências, critérios claros para determinar se uma vulnerabilidade deve ser divulgada e o mecanismo para administrar divergências dentro do comitê. Veja por exemplo: **https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.**

48 **GGE. 2021**, para. 61.

Tecnologia

Existem **capacidades técnicas específicas para identificar e resolver vulnerabilidades de** TIC relevantes para a aplicação da norma. Estas incluem, entre outras, ferramentas para a análise e avaliação de vulnerabilidade, para o compartilhamento de vulnerabilidades exploráveis (VEX)[49] e para **aplicação de patches em larga escala**, como software de gerenciamento de patches.

49 "O compartilhamento de vulnerabilidades e explorabilidade (VEX) é um sistema usado por produtores de software para compartilhar com consumidores de software uma avaliação das vulnerabilidades presentes em seus componentes de software. VEX é o mecanismo pelo qual os produtores de software classificam e rotulam vulnerabilidades em seus softwares. [...] Eles também incluem uma análise de vulnerabilidades; por exemplo, se a vulnerabilidade pode ou não ser explorável e por que, e como a vulnerabilidade pode ser mitigada ou corrigida, bem como quaisquer soluções alternativas conhecidas que podem ser usadas para protegê-la"; ver: **https://www.endorlabs.com/blog/what-is-vex-and-why-should-i-care**.

3.11 Norma K

Os Estados não devem conduzir ou apoiar intencionalmente atividades que danifiquem os sistemas de informação das equipes autorizadas de resposta a emergências (às vezes conhecidas como equipes de resposta a emergências informáticas ou equipes de resposta a incidentes de cibersegurança) de outro Estado. Um Estado não deve usar equipes de resposta a emergências autorizadas para se envolver em atividades internacionais maliciosas.

Políticas e Regulamentos

A fim de aplicar a norma corretamente, os Estados-membros devem definir a sua **posição sobre a norma** ou sobre determinados aspectos da norma. Por exemplo, é essencial definir a posição nacional sobre a aplicabilidade do direito internacional quanto ao uso das TICs pelos Estados e sobre os conceitos de "atividades internacionais maliciosas" e "apoio com conhecimento de causa". Recomenda-se que um Estado-membro, a fim de sinalizar à comunidade internacional seu compromisso com o cumprimento da norma, publique uma **declaração afirmando que não utilizará equipes autorizadas de resposta a emergências para se envolver em atividades internacionais maliciosas ou ofensivas.** Como um sinal para outros Estados, é igualmente importante que os Estado-membros declarem em **uma lista quais são todos os CSIRTs/CERTs em seu território**. A nível nacional, os Estados-membros devem descrever claramente na sua política ou estratégia de cibersegurança a **situação, autoridade e mandatos das suas CERT/CSIRT**, juntamente com o que distingue as suas funções únicas e neutras de outras funções governamentais. Finalmente, dado o papel neutro e único dessas equipes de detecção e resposta a incidentes cibernéticos, é importante estabelecer um **marco regulatório para o trabalho dos CERT/CSIRT que esteja alinhada com diretrizes e normas internacionais** (por exemplo, o código de ética FIRST ou ISO 27/2001).

Estruturas e Processos

Embora a norma não exija que os Estado-membros estabeleçam capacidades nacionais (ou regionais) de resposta a incidentes cibernéticos, como os recursos descritos na Norma A, recomenda-se que os Estado-membros **estabeleçam ou participem de um CSIRT/CERT regional nacional**. Por outro lado, tendo em conta o objetivo da norma, é importante que os Estados-membros estabeleçam **mecanismos de fiscalização independentes e eficazes** (judicial, administrativo, parlamentar), capazes de garantir a transparência e a responsabilização relativamente ao funcionamento do Estado no domínio das TIC (por exemplo, uma comissão parlamentar).

Associações e Redes

Este estudo não identificou quaisquer capacidades críticas, em termos de parcerias e redes, necessárias para implementar esta norma.

Pessoas e Habilidades

É muito importante que os Estado-membros sejam capazes de identificar e documentar possíveis casos de uso indevido dos CSIRT/CERT em atividades maliciosas. Por conseguinte, os Estados-membros devem dispor de **especialistas que efetuem a investigação técnica destas atividades** (por exemplo, analistas forenses de TIC) ou, caso a investigação técnica seja efetuada por terceiros, que possam avaliar a sua qualidade. Além disso, é importante que os **funcionários públicos** (incluindo os militares) **estejam cientes** do papel e do status dos CERT/CSIRT. Finalmente, o **conhecimento jurídico especializado, entre outras áreas do direito internacional específicas ao campo das TIC**, é fundamental para implementar adequadamente vários elementos (por exemplo, redigir a interpretação nacional da norma) relacionados com a implementação da norma.

Tecnologia

Este estudo não identificou nenhuma capacidade tecnológica crítica necessária para implementar esta norma.

4. Direito Internacional

O capítulo anterior apontou elementos específicos do direito internacional relevantes em normas específicas. Esta seção fornece uma descrição mais geral das FCC relacionadas ao direito internacional que vão além dos requisitos específicos das normas descritas acima. O relatório substantivo do OEWG 2019-2021 destaca que, "[re]conhecendo a Resolução 70/237 da Assembleia Geral e a Resolução 73/27 da Assembleia Geral, que estabeleceu o OEWG, os Estados reafirmaram que o direito internacional, e em particular a Carta das Nações Unidas, é aplicável e essencial para manter a paz e a estabilidade e promover TIC abertas, seguras, estáveis, acessíveis e pacíficas".[50]

Políticas e Regulamentos

Os Estado-membros concordaram que o direito internacional é aplicável às TICs e que "é necessário desenvolver entendimentos mais comuns sobre como aplicar o direito internacional ao uso estatal das TIC".[51] Para promover o desenvolvimento de um entendimento comum sobre como aplicar o direito internacional, recomenda-se que os Estado-membros desenvolvam e intercambiem

50 **OEWG. 2021. Final Substantive Report**, par. 3. 4.
51 Ibid.

seus respectivos pontos de vista. Como ponto de partida, os Estados devem desenvolver **posições públicas nacionais sobre a aplicabilidade do direito internacional no contexto das TIC**.

Estruturas e Processos

Recomenda-se que, a fim de assegurar que o comportamento dos Estado-membros no ciberespaço e seu uso das TIC seja legal, e para responsabilizá-los por suas ações, os Estado-membros estabeleçam (em nível nacional ou regional) um **mecanismo de supervisão independente** (judicial, administrativo, parlamentar).

Associações e Redes

Tendo em vista os desafios atuais relativos ao desenvolvimento de um entendimento comum sobre como aplicar o direito internacional ao uso das TIC, é importante que os Estados-membros proponham **mecanismos de cooperação** (por exemplo, compartilhamento de lições aprendidas, estabelecimento de programas de visitas para especialistas jurídicos, compartilhamento de informações) nas áreas de direito internacional e leis e políticas nacionais. Recomenda-se também que os Estado-membros **participem ativamente em processos multilaterais relacionados ao direito internacional no campo das TIC** (por exemplo, OEWG).

Pessoas e Habilidades

Aplicar o direito internacional no campo das TIC ou desenvolver uma visão nacional sobre o assunto exige que os Estados desenvolvam ou tenham **acesso a conhecimentos jurídicos especializados**. Também é essencial que os Estado-membros possam participar de **discussões regionais e internacionais sobre direito internacional**, o que inclui a interação com a comunidade acadêmica e a sociedade civil em geral. Recomenda-se que, nesses contextos, os juristas e especialistas possam participar de forma significativa das atividades realizadas em um idioma diferente da sua língua materna.

Tecnologia

Este estudo não identificou nenhuma capacidade tecnológica crítica necessária para implementar esta norma.

5. Medidas de Fortalecimento da Confiança

Tal como acontece com o direito internacional, as medidas específicas de construção de confiança para os normas foram mencionadas nas várias seções do Capítulo 3. Este capítulo fornece uma descrição mais geral de medidas adicionais de fortalecimento da confiança que os Estados devem considerar implementar em nível nacional. Como indicado pelo relatório substantivo do primeiro OEWG, "[A]s medidas de construção de confiança (MFCs), que incluem medidas de transparência, cooperação e estabilidade, podem ajudar a prevenir conflitos, evitar percepções e mal-entendidos e reduzir as tensões. Eles são uma expressão concreta da cooperação internacional."[52] O relatório descreve os FCC relacionadas às MFC.

Políticas e Regulamentos

Em termos de políticas e normas para a promoção da transparência, recomenda-se que os Estados-membros **divulguem publicamente todas as estratégias, políticas e regulamentos nacionais de cibersegurança relevantes**, de preferência com uma tradução

52 **OEWG. 2021. Final Substantive Report**, par. 41.

oficial em inglês (no mínimo) para facilitar o acesso a eles. Por outra parte, é importante que os Estados-membros **identifiquem e considerem as MFCs adequadas ao seu contexto específico** e adoptem políticas e regulamentos para cooperar na sua aplicação com outros Estados (por exemplo, adoptem modelos para a partilha de informações ou estabeleçam pontos de contacto a nível nacional).

Estruturas e Processos

O estabelecimento de um ponto de contato é um dos elementos essenciais na construção da confiança. O estabelecimento de pontos de contacto a nível técnico e diplomático é importante para garantir a comunicação direta entre os Estados-membros, aspeto fundamental não só no que diz respeito à implementação de normas específicas, mas sobretudo em momentos de crise. Além disso, para promover a transparência, a cooperação e a estabilidade, os Estados-membros devem desenvolver **capacidades nacionais ou regionais de resposta a incidentes cibernéticos (por exemplo, um CERT/CSIRT).** Devido ao seu papel de "primeira resposta", essas estruturas desempenham um papel crítico ao lidar com incidentes ou ameaças logo que estes ocorrem. E muitas vezes isso significa interagir com seus homólogos no exterior. Na sua vez, essas interações contribuem para aumentar a transparência e a cooperação. Em termos de processos, é muito importante que os Estado-membros **compartilhem informações e boas práticas sobre vários tópicos relacionados**, incluindo ameaças e incidentes de TIC existentes e emergentes, normas para análise de vulnerabilidade de produtos de TIC, bem como a compartilhamento de informações sobre abordagens nacionais para Segurança de TIC e proteção de dados. Para tanto, os Estado-membros podem usar o Portal de Políticas Cibernéticas do Instituto das Nações Unidas para Pesquisa de Desarmamento.[53]

Associações e Redes

Medidas de fortalecimento da confiança podem ser implementadas desde que os Estado-membros se envolvam com outros em ambientes internacionais. Portanto, recomenda-se que os Estado-membros **participem dos processos das Nações Unidas** (como o GAWG, que tem sido reconhecido como uma medida de construção de confiança), em **diálogos bilaterais, sub-regionais, regionais e multilaterais**, e interajam com os **organismos regionais que desenvolveram e implementaram as MFCs**. Além disso, é muito importante que os Estado-membros **participem de marcos de cooperação entre CERT/CSIRT** ou outros órgãos técnicos de segurança, como a rede FIRST ou outros quadros regionais. Estes marcos oferecem uma oportunidade única de desenvolver relações de confiança dentro da comunidade técnica.

Pessoas e Habilidades

Os Estado-membros devem manter especialistas com **conhecimento das MFCs** e maneiras de ativá-los ou aproveitá-los em tempos de crise. Em particular, dado o papel fundamental dos PoCs, recomenda-se ter **pessoal treinado para atuar efetivamente como PoCs** (por exemplo, fornecer treinamento sobre a função e os processos do PoC). É também importante que os Estado-membros

53 https://cyberpolicyportal.org/.

disponham de pessoal capaz **de fazer uso de plataformas de partilha de informação** (por exemplo, o portal de políticas cibernéticas da UNIDIR), que são consideradas ferramentas importantes para promover a transparência. Finalmente, construir confiança requer funcionários públicos com **habilidades de comunicação e diplomáticas** que possam interagir com seus homólogos em debates sobre cibersegurança.

Tecnologia

Canais e plataformas de comunicação confiáveis entre os Estados são importantes para construir a confiança nas relações.

6. Conclusões

Como o cenário de ameaças cibernéticas está em constante evolução, é importante que os Estados maximizem sua capacidade de prevenir ou mitigar as consequências de atos maliciosos envolvendo TIC. Como parte desse esforço, conseguir implementar o Marco de Comportamento Responsável dos Estados no ciberespaço é um passo importante para aumentar a resiliência cibernética nacional como também um passo necessário para garantir a paz e a segurança no campo das TICs.
As principais capacidades cibernéticas fundamentais identificadas neste relatório pretendem representar as condições iniciais a partir das quais podem ser desenvolvidas medidas mais elaboradas ou avançadas. No entanto, a lista de capacidades identificadas não deve ser considerada fechada ou definitiva. Dados os desenvolvimentos contínuos e rápidos no campo das TIC (por exemplo, adoção generalizada de novas tecnologias disruptivas, como inteligência artificial ou computação quântica), elementos adicionais podem se tornar relevantes e fundamentais para as normas existentes ou para o desenvolvimento de novas normas.

Deve-se notar que, embora o objetivo deste estudo não seja classificar ou atribuir “pesos” específicos a FCC ou normas individuais, uma análise da distribuição geral de FCCs sugere que cinco elementos-chave emergem como particularmente proeminentes:

a. uma estratégia ou política nacional abrangente de cibersegurança;
b. uma entidade dedicada a atuar como elo ou entidade ou coordenador nacional em assuntos cibernéticos;
c. a capacidade de resposta a emergências ou incidentes (nacionais ou regionais);
d. cooperação bem estruturada entre todas as partes interessadas relevantes, incluindo o setor privado e operadores de infraestrutura crítica; e
e. acesso a habilidades especializadas (por exemplo, técnicas, jurídicas, diplomáticas, comunicação).

Esses cinco elementos principais estão entre os recursos mais recorrentes e relevantes em quase todos os componentes do Marco. Portanto, ao desenvolver esses elementos, os Estado-membros podem se beneficiar da implementação de todo o Marco. Além disso, tal como referido no Capítulo 2, é muito importante que os Estado-membros, ao implementar capacidades cibernéticas fundamentais, o façam com total respeito pelos direitos humanos e levando em conta as dimensões de gênero. Esforços futuros de pesquisa podem desagregar ainda mais cada pilar ou elemento do FCC, a fim de aprofundar a compreensão da atual dinâmica de gênero e enquadrar melhor sua formulação e implementação.

As FCC apresentadas neste relatório constituem os elementos por meio dos quais os Estado-membros podem implementar o Marco e promover a paz, segurança, cooperação e confiança internacionais no ambiente das TIC. A segunda parte deste estudo, intitulada “Introdução a uma abordagem baseada em ameaças”, propõe uma abordagem que permitiria aos governos avaliar melhor sua prontidão para aproveitar as vantagens do Marco e prevenir ou responder a atividades e ameaças maliciosas específicas relacionadas com as TIC.

Anexo 1. Tabela de Capacidades Cibernéticas Fundamentais

Norma A

Os Estados devem cooperar no desenvolvimento e aplicação de medidas para aumentar a estabilidade e segurança no uso das TIC e prevenir práticas de TIC reconhecidas como nocivas ou que possam representar uma ameaça à paz e segurança internacionais.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Política e estratégia de cibersegurança (e plano de implementação nacional) ou legislação nacional de cibersegurança (de preferência com uma abordagem de todo o governo).
iii	Abordagem de gestão de riscos cibernéticos (incluindo infraestruturas críticas).
iv	Política externa que reconhece a cibersegurança como uma das prioridades.
v	Compromisso público com o Marco de Comportamento Responsável dos Estados no ciberespaço.
vi	Declaração pública sobre capacidades cibernéticas nacionais disponível (informação não classificada).
vii	Estratégias e planos nacionais para o desenvolvimento de competências cibernéticas.
ESTRUTURAS E PROCESSOS	
i	Centro nacional, agência ou entidade responsável pela cibersegurança.
ii	Capacidades nacionais ou regionais de detecção e resposta a incidentes cibernéticos (por exemplo, CERT/CSIRT ou um Centro de Operações de Segurança).
iii	Ponto de contato (PoC) a nível diplomático e técnico.
iv	Cooperação e compartilhamento de informações entre a legislação e a aplicação da lei.
v	Mecanismos de supervisão independentes e eficazes (judicial, administrativo, parlamentar) capazes de garantir a transparência e a responsabilização relativamente ao funcionamento do Estado no âmbito das TIC.
ASSOCIAÇÕES E REDES	
i	Cooperação intrasetorial (setor privado, sociedade civil, comunidade técnica, academia).
ii	Cooperação intragovernamental (por exemplo, reuniões interministeriais, grupos de trabalho).
iii	Cooperação bilateral, regional e multilateral em diferentes níveis (técnico, operacional, diplomático).
iv	Acordos multilaterais (por exemplo, a Convenção de Budapeste, a Convenção de Malabo).
PESSOAS E HABILIDADES	
i	Capacidades diplomáticas para participar em processos internacionais e intergovernamentais.
ii	Especialistas e profissionais de políticas com conhecimento básico de cibersegurança.
iii	Juristas com competências jurídicas em direito internacional relacionadas com atividades no âmbito das TIC.
iv	Programas de “formação de formadores” e certificação profissional.
v	Competências para gerir incidentes de cibersegurança, incluindo preparação, resposta e recuperação, tanto a nível nacional como internacional.
vi	Campanhas sistemáticas de sensibilização, dirigidas ao público em geral, sobre a importância dos patches de segurança e outras práticas básicas de ciber-higiene como as atualizações de software.
TECNOLOGIA	
i	Capacidades para garantir a cibersegurança nos pontos terminais (antivírus ou atualizações automáticas e patches de produtos digitais para mitigar erros e vulnerabilidades de segurança).
ii	Capacidades técnicas para prevenir, detectar ou interromper atos maliciosos relacionados com as TIC.
iii	Soluções técnicas para proteger as comunicações (por exemplo, criptografia).

Norma B

No caso de incidentes de TIC, os Estados devem considerar todas as informações relevantes, incluindo o contexto mais amplo do evento, as dificuldades de atribuição no ambiente de TIC e a natureza e extensão das consequências.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Posição(ões) ou declaração(ões) nacional(is) sobre a aplicação do direito internacional ao uso das TIC pelos Estados.
iii	Classificação (pública ou não pública) de incidentes de TIC em termos de escala e impacto.
iv	Política de atribuição (pública ou não pública) que inclui definições, metodologia e funções e responsabilidades claras.
v	Regulamento que permite a compartilhamento de informações com entidades comerciais relevantes e outras entidades não governamentais.
ESTRUTURAS E PROCESSOS	
i	Critérios de evidência nacional para determinar a atribuição.
ii	Processos e procedimentos que permitem o compartilhamento de informações entre as entidades governamentais e não governamentais relevantes.
ASSOCIAÇÕES E REDES	
i	Cooperação entre as partes interessadas nacionais (por exemplo, grupos de trabalho, plataformas de múltiplas partes interessadas.
ii	Cooperação bilateral e multilateral em questões de assistência internacional e compartilhamento de informações.
iii	Cooperação bilateral e multilateral para a solução de divergências e controvérsias por meio de consultas e outros meios pacíficos.
PESSOAS E HABILIDADES	
i	Habilidades para realizar (ou avaliar, se a informação for fornecida por terceiros) investigações técnicas de incidentes de TIC.
ii	Funcionários públicos (incluindo pessoal diplomático) com competências jurídicas específicas no contexto das TIC, incluindo consultas e outros meios pacíficos para resolver disputas à escala internacional.
iii	Funcionários públicos (incluindo funcionários diplomáticos) com habilidades de negociação e comunicação específicas para o contexto de TIC.
TECNOLOGIA	
i	Capacidades técnicas e forenses para investigar e determinar a origem da atividade maliciosa relacionada às TIC.

Norma C

Os Estados não devem permitir conscientemente que seu território seja usado para cometer atos internacionalmente ilícitos usando as TIC.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma, incluindo a opinião do Estado sobre o que constitui ato internacionalmente ilícito de uso das TIC.
ii	Estratégia e política de cibersegurança, incluindo disposições para prevenir, detectar e interromper o uso malicioso de TIC.
iii	Legislação específica que define quais tipos de atividades de TIC são e não são permitidas no território e que outorga autoridade para investigar, encerrar ou processar esses tipos de atividades.
ESTRUTURAS E PROCESSOS	
i	Capacidades nacionais ou regionais de detecção e resposta a incidentes cibernéticos (por exemplo, CERT/CSIRT ou um Centro de Operações de Segurança).
ii	Capacidade de aplicação da lei cibernética.
iii	Procedimento para compartilhamento de informações entre as partes interessadas nacionais relevantes, incluindo entidades não governamentais.
iv	Mecanismos para enviar ou responder a solicitações de assistência (incluindo procedimentos para avaliar solicitações).
ASSOCIAÇÕES E REDES	
i	Cooperação entre as partes interessadas nacionais (por exemplo, grupos de trabalho, plataformas de múltiplas partes interessadas), incluindo parcerias público-privadas relevantes.
ii	Acordos bilaterais e multilaterais sobre questões de assistência e compartilhamento de informações.
iii	Marco para compartilhamento de informações em nível técnico (como a rede FIRST).
PESSOAS E HABILIDADES	
i	Capacidade de identificar e interromper atos maliciosos que usam TIC alocados em seu próprio território.
ii	Funcionários públicos (incluindo pessoal diplomático) com competências de comunicação específicas para o contexto das TIC.
TECNOLOGIA	
i	Capacidade técnica para prevenir, detectar ou interromper atos maliciosos relacionados com as TIC alocados no seu próprio território.

Norma D

Os Estados devem considerar a melhor forma de cooperar para o compartilhamento de informações, prestarem assistência mútua, processar o uso terrorista e criminoso das TIC e implementar outras medidas de cooperação para enfrentar esse tipo de ameaça.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Assinatura e ratificação de instrumentos bilaterais, regionais ou multilaterais sobre crimes cibernéticos.
iii	Políticas que descrevam os mecanismos ou procedimentos de cooperação e compartilhamento de informações, que devem incluir entidades comerciais e outras entidades não governamentais relevantes.
iv	Legislação sobre crimes cibernéticos que garante uma abordagem tecnologicamente neutra.
ESTRUTURAS E PROCESSOS	
i	Mecanismo de envio ou resposta a pedidos de assistência (por exemplo, pedidos de assistência jurídica mútua).
ii	Protocolos e procedimentos para coletar, tratar e armazenar evidências digitais.
iii	Capacidade de aplicação da lei cibernética.
iv	Recursos nacionais ou regionais de detecção e resposta a incidentes cibernéticos (por exemplo, CERT/CSIRT ou um Centro de Operações de Segurança).
ASSOCIAÇÕES E REDES	
i	Cooperação bilateral, regional e multilateral para investigação, assistência, aplicação da lei e compartilhamento de informações sobre o uso criminoso e terrorista das TIC (por exemplo, tratados de assistência jurídica mútua).
ii	Redes operacionais (por exemplo, INTERPOL I-24/7) e técnicas (por exemplo, FIRST).
iii	Cooperação entre as partes interessadas nacionais relevantes (por exemplo, grupos de trabalho, plataformas multissetoriais), inclusive por meio de parcerias público-privadas estruturadas.
PESSOAS E HABILIDADES	
i	Capacidade de lidar com evidências digitais a nível técnico e legal.
ii	Conhecimento da legislação sobre cibercrime e terrorismo em outros Estados-membros.
iii	Capacidade de construir relacionamentos com contrapartes e parceiros bilaterais, regionais e internacionais para garantir que as intervenções sejam eficientes e oportunas.
TECNOLOGIA	
i	Capacidade técnica para prevenir, detectar ou interromper atos maliciosos relacionados às TIC por criminosos e terroristas.
ii	Canais de comunicação ou plataformas seguras para compartilhar informações.

Norma E

Os Estados, ao garantir o uso seguro das TIC, devem garantir o pleno respeito aos direitos humanos, incluindo o direito à liberdade de expressão.

POLÍTICAS E REGULAMENTOS	
i	Posição nacional sobre como o direito internacional é aplicado, incluindo o direito internacional dos direitos humanos.
ii	Políticas e estratégias de cibersegurança consistentes com a lei internacional de direitos humanos (por exemplo, orientação nas resoluções 68/167 e 69/166).
iii	Não imponha restrições indevidas à liberdade de expressão e à liberdade de procurar, receber e transmitir informações.
iv	Regulamentos, inclusive para empresas, relativas ao respeito aos direitos humanos na concepção, desenvolvimento e uso de novas tecnologias.
v	Legislação sobre vigilância e interceptação pelo Estado, de acordo com o direito à privacidade.
vi	Leis de proteção de dados.
ESTRUTURAS E PROCESSOS	
i	Mecanismos de fiscalização nacionais ou regionais independentes e eficazes (judicial, administrativo ou parlamentar) capazes de garantir a transparência e a responsabilização relativamente à vigilância das comunicações, interceptação e coleta de dados pessoais pelo Estado.
ASSOCIAÇÕES E REDES	
i	Participar e consultar as partes interessadas que defendem, promovem e analisam os direitos humanos e as liberdades fundamentais online para entender e minimizar os possíveis impactos negativos das políticas sobre os indivíduos.
PESSOAS E HABILIDADES	
i	Funcionários públicos (incluindo aqueles que trabalham na aplicação da lei) com conhecimento de direitos humanos no âmbito digital, bem como de como implementar instrumentos internacionais de maneira consistente com os direitos humanos.
ii	Conhecimentos especializados sobre direitos humanos e contextualizados, inclusive na área jurídica.
TECNOLOGIA	
i	Capacidade tecnológica para garantir o respeito aos direitos humanos no uso das TIC por atores estatais e não estatais.

Norma F

Um Estado não deve conduzir ou apoiar conscientemente uma atividade de TIC contrária às suas obrigações ao abrigo do direito internacional que intencionalmente danifique ou prejudique a infraestrutura crítica.

POLÍTICAS E REGULAMENTOS	
i	Posição nacional sobre a aplicabilidade do direito internacional no uso das TIC pelos Estados.
ii	Interpretação nacional da norma.
iii	Classificação (pública ou não pública) de incidentes de TIC em termos de escala e gravidade.
iv	Concepção nacional de infraestrutura crítica.
ESTRUTURAS E PROCESSOS	
i	Mecanismos de supervisão nacionais ou regionais independentes e eficazes (judicial, administrativo, parlamentar) capazes de garantir a transparência, conforme o caso.
ASSOCIAÇÕES E REDES	
i	Marcos de cooperação bilateral, regional e multilateral para cooperação e compartilhamento de informações.
PESSOAS E HABILIDADES	
i	Conhecimento especializado do direito internacional aplicável especificamente às atividades desenvolvidas no âmbito das TIC.
TECNOLOGIA	
N/D	

Norma G

Os Estados devem tomar medidas apropriadas para proteger sua infraestrutura crítica contra ameaças relacionadas às TIC.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Designação nacional de setores de infraestrutura críticos.
iii	Classificação (pública ou não pública) de incidentes de TIC em termos de escala e gravidade.
iv	Legislação para proteção de infraestrutura crítica (estabelecimento de normas, relatórios, auditorias etc.).
v	Estratégia e política de cibersegurança que inclui disposições sobre redução de risco cibernético em infraestrutura crítica e medidas de cibersegurança para produtos de TIC, e que leva em consideração a resolução 58/199 sobre a cultura global de cibersegurança e proteção de infraestrutura crítica de informação.
vi	Regulamento que permite a compartilhamento de informações com entidades comerciais relevantes e outras entidades não governamentais.
ESTRUTURAS E PROCESSOS	
i	Centro(s) ou agência(s) nacional(is) responsável(is) pela infraestrutura crítica.
ii	ii. Capacidades nacionais ou regionais de detecção e resposta a incidentes cibernéticos (por exemplo, CERT/CSIRT ou um Centro de Operações de Segurança).
iii	Mecanismos de cumprimento das medidas de cibersegurança na infraestrutura crítica.
iv	Planos de contingência em caso de incidentes de TIC que envolvam infraestrutura crítica.
v	Processos e procedimentos que permitem o compartilhamento de informações entre as entidades governamentais e não governamentais relevantes.
ASSOCIAÇÕES E REDES	
i	Cooperação transfronteiriça com operadores e proprietários de infraestrutura relevante (por exemplo, coordenação de respostas a incidentes, compartilhamento de boas práticas de proteção de dados, infraestrutura crítica).
ii	Cooperação entre partes interessadas nacionais relevantes (por exemplo, comitês interinstitucionais, plataformas multissetoriais), incluindo parcerias público-privadas e proprietários, operadores ou administradores de propriedade de infraestrutura crítica.
PESSOAS E HABILIDADES	
i	Habilidades técnicas para proteger a infraestrutura crítica nacional contra atos maliciosos envolvendo TIC.
ii	Treinamentos e exercícios que visam melhorar a capacidade de resposta e testar a continuidade dos serviços e planos de contingência para ataques a infraestruturas críticas e que estimulem os interessados a participar de atividades similares.
iii	Pessoal diplomático com capacidade para **interagir significativamente com seus homólogos sobre o tema específico das infraestruturas críticas**, especialmente se estas forem transnacionais.
TECNOLOGIA	
i	Capacidade técnica para prevenir, detectar ou interromper atos maliciosos contra infraestruturas críticas relacionadas com as TIC.

Norma H

Os Estados devem responder às solicitações apropriadas de assistência de outro Estado cuja infraestrutura crítica esteja sujeita a atos maliciosos de TIC.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Legislação que fornece um marco para solicitar e fornecer assistência internacional.
iii	Estratégias e políticas de cibersegurança que descrevem os mecanismos, procedimentos e processos para responder a solicitações de assistência.
ESTRUTURAS E PROCESSOS	
i	Mecanismos eficientes para receber, processar, avaliar e responder aos pedidos de assistência, bem como para os preparar e enviar.
ii	Capacidade de aplicação da lei cibernética.
ASSOCIAÇÕES E REDES	
i	Cooperação bilateral, regional e multilateral para a proteção de infraestrutura crítica (por exemplo, criação de modelos comuns para solicitação de assistência, assinatura de Memorandos de Entendimento etc.).
ii	Cooperação transfronteiriça com os principais proprietários e operadores de infraestrutura, bem como provedores (por exemplo, coordenação de sistemas de alerta de emergência e compartilhamento e análise de informações de vulnerabilidade).
iii	Cooperação entre as partes interessadas relevantes (por exemplo, parcerias público-privadas e comissões interinstitucionais).
PESSOAS E HABILIDADES	
i	Capacidade de fornecer assistência transfronteiriça eficaz e oportuna aos Estados que estão sob ataque contra infraestrutura crítica.
ii	Habilidades para atender e gerir pedidos de assistência.
TECNOLOGIA	
i	Capacidade técnica para prevenir, detectar ou interromper atos maliciosos contra infraestruturas críticas relacionadas com as TIC.
ii	Canais de comunicação ou plataformas seguras para compartilhamento de informações relacionadas a atos maliciosos contra infraestruturas críticas que envolvam TIC.

Norma I

Os Estados devem tomar medidas razoáveis para garantir a integridade da cadeia de abastecimento e tentar impedir a proliferação de ferramentas e técnicas de TIC maliciosas e o uso de funções nocivas ocultas.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Leis e regulamentos que proíbem a introdução de funções ocultas prejudiciais e a exploração de vulnerabilidades em produtos de TIC.
iii	Política e estratégia de cibersegurança que abranja a segurança da cadeia de abastecimento e descreva marcos importantes.
iv	Obrigação de implementar regras e normas comuns globalmente interoperáveis para segurança da cadeia de abastecimentos (por exemplo, ISO/IEC 20243).
v	Exigir que os provedores incorporem segurança e proteção no gerenciamento do ciclo de vida de seus produtos de TIC.
ESTRUTURAS E PROCESSOS	
i	Mecanismo de governança para gestão de riscos na cadeia de abastecimento, que deve incluir os atores-chave que representam os nós da cadeia de valor.
ii	Mecanismo de avaliação e certificação de produtos TIC (nacionais ou em aliança com outros países).
iii	Acordos para garantir a interoperabilidade de abordagens, métodos de certificação e certificações de produtos de TIC entre jurisdições.
ASSOCIAÇÕES E REDES	
i	Medidas de cooperação a nível bilateral, regional e multilateral para, por exemplo, o compartilhamento de boas práticas de gestão de riscos na cadeia de abastecimento ou a certificação de produtos TIC.
PESSOAS E HABILIDADES	
i	Capacidades em questões de segurança e gestão de riscos da cadeia de abastecimento.
ii	Habilidades de resposta e gerenciamento de incidentes.
iii	Pessoal diplomático com capacidade para **interagir significativamente com seus homólogos sobre o tema específico das infraestruturas críticas**, especialmente se estas forem transnacionais.
TECNOLOGIA	
i	Capacidade técnica para prevenir, detectar ou interromper ataques às cadeias de abastecimento.

Norma J

Os Estados devem encorajar a notificação responsável de vulnerabilidades de TIC e compartilhar as informações correspondentes sobre soluções disponíveis para essas vulnerabilidades, a fim de limitar e possivelmente eliminar ameaças potenciais às TIC e à infraestrutura dependente de TIC.

POLÍTICAS E REGULAMENTOS	
i	Interpretação nacional da norma.
ii	Medidas legais para impedir a distribuição comercial de vulnerabilidades.
iii	Descriminalização e proteção legal para pesquisadores de segurança e *hackers* éticos que desejam expor vulnerabilidades.
iv	Política de divulgação de vulnerabilidade coordenada (CVD).
v	Marcos jurídicos que permitem a cooperação e o compartilhamento de informações com vendedores e provedores.
vi	vRequisitos que uma política e prática de gestão de vulnerabilidade eficiente e eficaz devem atender.
ESTRUTURAS E PROCESSOS	
i	Orientação sobre as respectivas funções e responsabilidades das diferentes partes interessadas nos processos de notificação de vulnerabilidade, incluindo os tipos de informações técnicas a serem divulgadas e tratamento de dados confidenciais etc.
ii	Protocolos estabelecidos para comunicação e compartilhamento de informações entre todas as partes interessadas relevantes (por exemplo, governos, vendedores e provedores, pesquisadores de segurança, equipes de resposta a incidentes). Protocolos estabelecidos para atualização e patching de sistemas, particularmente aqueles relacionados a infraestruturas dependentes de TIC.
iii	Orientação e incentivos para divulgação coordenada de vulnerabilidades (por exemplo, programas de recompensas por detecção de erros).
iv	Campanhas sistemáticas de conscientização (dirigidas tanto ao público em geral quanto a profissionais de setores específicos, principalmente aqueles que atuam em setores de infraestrutura crítica) sobre a importância dos patches de segurança.
ASSOCIAÇÕES E REDES	
i	Cooperação bilateral, regional e multilateral para a divulgação de vulnerabilidades.
ii	Cooperação intersetorial com o setor privado, sociedade civil e comunidade técnica, incluindo provedores e proprietários.
PESSOAS E HABILIDADES	
i	Habilidades técnicas para identificar e resolver vulnerabilidades ou gerenciar informações relacionadas a vulnerabilidades recebidas de terceiros (por exemplo, empresas que oferecem recompensas por detecção de erros, pesquisadores de segurança, provedores).
ii	Habilidades de comunicação pública necessárias para lidar com vulnerabilidades, especialmente quando elas têm impacto na população em geral.
iii	Habilidades diplomáticas e de comunicação necessárias para poder participar com sucesso em discussões de gerenciamento de vulnerabilidade com atores estatais e não estatais relevantes.
TECNOLOGIA	
i	Capacidade técnica para identificar e resolver vulnerabilidades de TIC ou para agir quando a informação é fornecida por terceiros.
ii	Capacidade técnica para instalar patches de grande escala.

Norma K

Os Estados não devem conduzir ou apoiar intencionalmente atividades que danifiquem os sistemas de informação das equipes autorizadas de resposta a emergências (às vezes conhecidas como equipes de resposta a emergências informáticas ou equipes de resposta a incidentes de cibersegurança) de outro Estado. Um Estado não deve usar equipes de resposta a emergências autorizadas para se envolver em atividades internacionais maliciosas.

POLÍTICAS E REGULAMENTOS	
i	Posição nacional sobre a norma (ou certos aspectos dela).
ii	Declaração pública de que o Estado não utilizará equipes autorizadas de resposta a emergências para participar de atividades internacionais maliciosas ou ofensivas e que respeitará os princípios éticos que norteiam o trabalho dessas organizações.
iii	Lista de todos os CERT/CSIRT declarados.
iv	Política ou estratégia de cibersegurança que descreve claramente o status (por exemplo, infraestrutura crítica), autoridade e mandatos de CERTs/CSIRTs, juntamente com o que distingue suas funções únicas e neutras de outras funções governamentais.
v	Marco regulamentar para o trabalho dos CERTs/CSIRTs alinhado com as diretrizes e normas internacionais (por exemplo, o código de ética FIRST ou ISO 27/2001).
ESTRUTURAS E PROCESSOS	
i	Capacidades nacionais ou regionais de resposta a incidentes cibernéticos (por exemplo, CERTs/CSIRTs ou um Centro de Operações de Segurança).
ii	Mecanismos de supervisão independentes e eficazes (judicial, administrativo, parlamentar) capazes de garantir a transparência e a responsabilização relativamente ao funcionamento do Estado no domínio das TIC.
ASSOCIAÇÕES E REDES	
N/D	
PESSOAS E HABILIDADES	
i	Habilidades para conduzir (ou avaliar, se as informações forem fornecidas por terceiros) investigações técnicas sobre o uso indevido do CERT ou CSIRT para conduzir atividades maliciosas.
ii	Funcionários públicos (incluindo militares) cientes do papel e status dos CERT/CSIRT.
iii	Conhecimento especializado sobre direito internacional aplicável especificamente no âmbito das TIC.
TECNOLOGIA	
N/D	

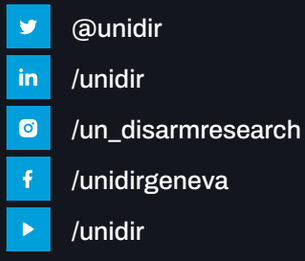
Direito Internacional

Observação: esta seção da tabela da FCC inclui elementos adicionais da lei internacional que devem ser considerados complementares ou suplementares àqueles especificamente incluídos em cada regra.

POLÍTICAS E REGULAMENTOS	
i	Declaração pública de como o Estado entende a aplicação do direito internacional ao ciberespaço.
ESTRUTURAS E PROCESSOS	
i	Mecanismos de fiscalização independentes (judicial, administrativo, parlamentar) capazes de garantir a legalidade e a responsabilização relativamente às operações do Estado no âmbito das TIC.
ASSOCIAÇÕES E REDES	
i	Cooperação com outros Estado-membros nas áreas de direito internacional, legislação e políticas nacionais.
ii	Participação em processos multilaterais relacionados com o direito internacional na área das TIC.
PESSOAS E HABILIDADES	
i	Conhecimento especializado em direito internacional eas responsabilidades dos Estados no âmbito cibernético.
ii	Capacidade de participar de discussões regionais e internacionais sobre direito internacional, incluindo a capacidade de interagir com a comunidade acadêmica e a sociedade civil em geral, em um idioma que pode não ser a língua materna.
TECNOLOGIA	
N/D	

Medidas de Construção de Confiança

POLÍTICAS E REGULAMENTOS	
i	Divulgação pública de todas as estratégias, políticas e regulamentos nacionais de cibersegurança relevantes, de preferência com uma tradução oficial para o inglês (no mínimo) para facilitar o acesso e a transparência.
ii	Identificar e considerar MFC apropriados em seus contextos específicos e cooperar com outros Estados em sua implementação.
ESTRUTURAS E PROCESSOS	
i	Estabelecimento de Pontos de Contacto (PoC) nacionais ao nível diplomático e técnico.
ii	Capacidades nacionais ou regionais de resposta a incidentes cibernéticos (por exemplo, CERT/CSIRT ou um Centro de Operações de Segurança).
iii	Compartilhar informações e boas práticas, lições ou livros brancos sobre: • ameaças e incidentes existentes e emergentes relacionados à segurança de TIC; • estratégias e normas nacionais para a análise de vulnerabilidades em produtos de TIC; • abordagens nacionais e regionais para gestão de riscos e prevenção de conflitos.
iv	Compartilhamento de informações sobre: • abordagens nacionais para segurança de TIC; • proteção de dados; • proteção de infraestrutura crítica dependente de TIC; • a missão e funções do órgão responsável pela segurança das TIC, a estratégia de TIC a nível nacional ou organizacional e os regimes legais e de supervisão em que operam.
ASSOCIAÇÕES E REDES	
i	Participação em processos das Nações Unidas (por exemplo, OEWG).
ii	Participar do diálogo por meio de consultas bilaterais, sub-regionais, regionais e multilaterais.
iii	Participar em/com órgãos regionais que desenvolvem e implementam as MFCs.
iv	Participar de estruturas de cooperação entre CERT/CSIRT ou outros órgãos técnicos de segurança, como a rede FIRST ou outros marcos regionais.
PESSOAS E HABILIDADES	
i	Conhecimento das MFCs existentes e formas de ativá-los ou aproveitá-los em tempos de crise.
ii	Conhecimento e competências necessários para atuar efetivamente como PoC nacional (se nomeado).
iii	Capacidade de fazer uso de plataformas de compartilhamento de informações existentes (por exemplo, portal de políticas cibernéticas UNIDIR).
iv	Habilidades diplomáticas e de comunicação necessárias para participar efetivamente em debates sobre cibersegurança com seus homólogos em outros países.
TECNOLOGIA	
i	Canais e plataformas confiáveis de comunicação entre os Estados.



Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG